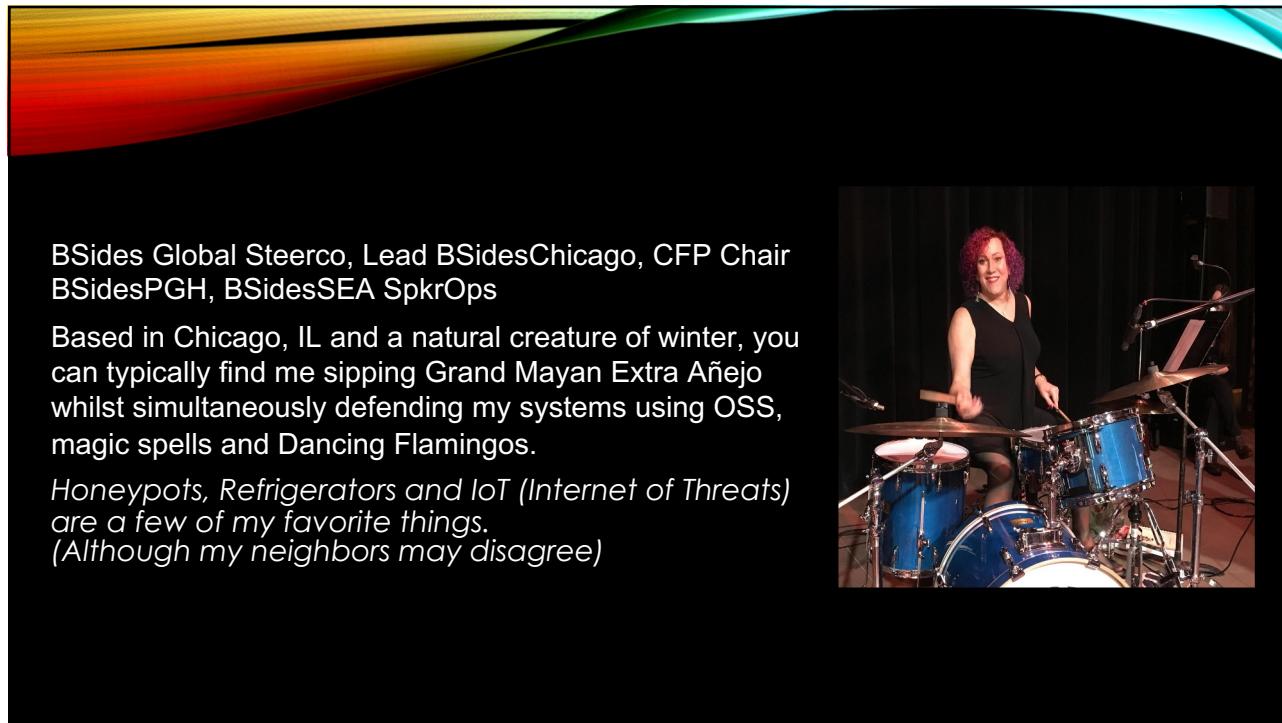




1



2

DISCLAIMER

- I'm obsessed(?) with home security lab equipment, honeypots and colos
- If you want to have a life, perhaps tone it down a bit

4

Why Are We Here!

- Security is fun
- Toys are fun
- I like breaking things
- I like building things
 - I like breaking things I build
- Learning never ends



6

SOME BASICS

Your Lab!

- Virtualize
 - Proxmox - proxmox.com/en
 - Virtualbox – virtualbox.org
 - UTM - github.com/utmapp/UTM
- Pis
 - OpenWRT - openwrt.org
 - OpnSense - opnsense.org

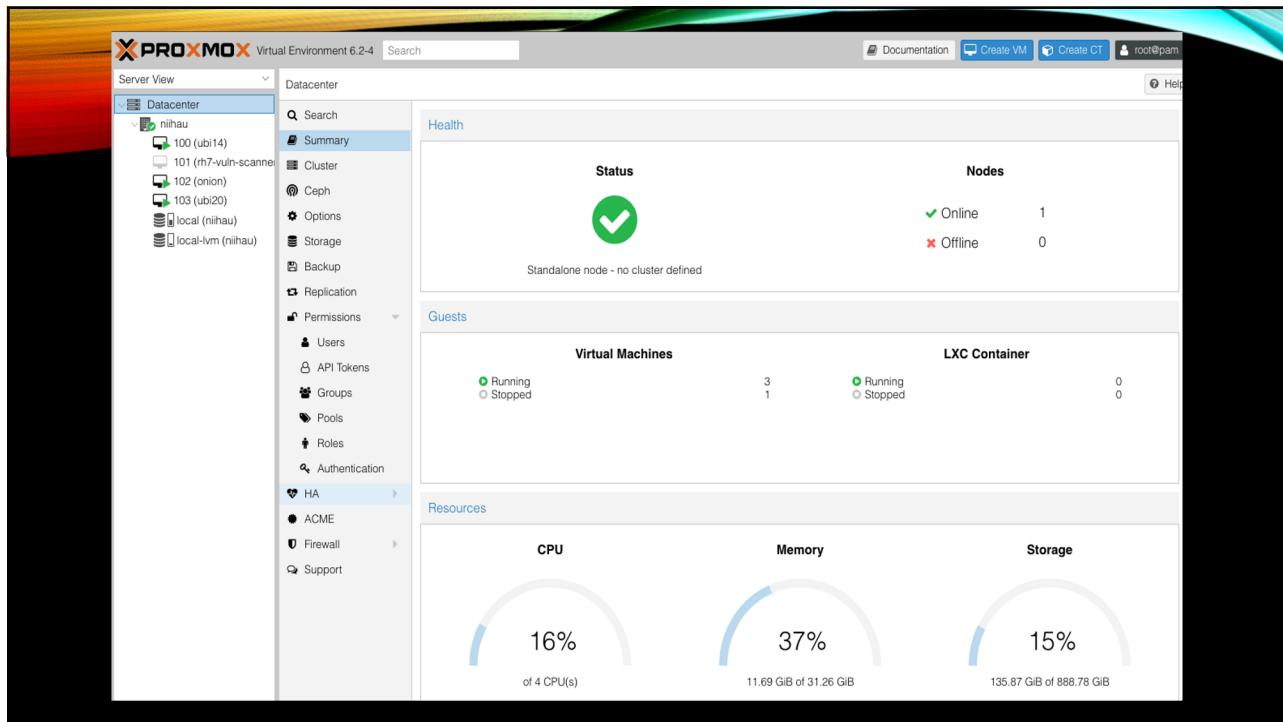


7

VIRTUALIZE!



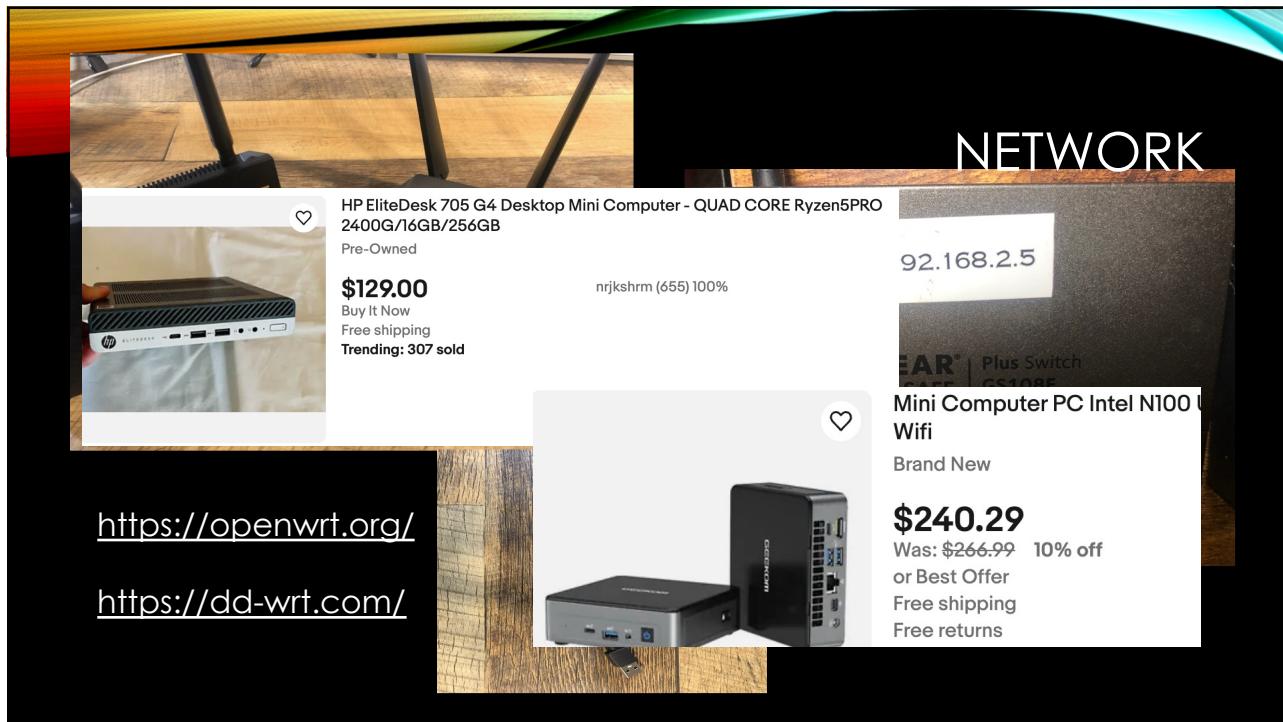
8



9



10



11



12



13

OK – NOW WHAT?

- Install all the things!
- OSes come in all shapes and sizes
- Ollama! ollama.com
- Don't forget Windoze
 - www.microsoft.com/en-us/evalcenter/
 - Snapshots (180 days)
- Monitoring!!! (Wazuh - more in a minute)

Get up and running with large language models.

Run [Llama 3](#), [Phi 3](#), [Mistral](#), [Gemma 2](#), and other models. Customize and create your own.

Download ↓

14

LLaMA + Suricata logs

- Install Ollama
 - curl -fsSL https://ollama.com/install.sh | sh

```
echo "Summarize these Suricata logs. Focus on unusual traffic or patterns." | \
cat - <(tail -n 100 /var/log/suricata/eve.json) | ollama run llama3
```

Between 14:00 and 14:10 UTC, host 192.168.1.42 generated over 100 DNS queries to subdomains of dns.exfiltrator.org.

Many of the query names contained unusually long, base64-encoded strings, suggesting DNS tunneling activity.

The destination was a public resolver (208.110.32.27) and not a local DNS server.

Behavior is consistent with low-rate data exfiltration via DNS covert channel.

Recommendation: Isolate host, investigate process making queries, and block outbound DNS to untrusted domains.

15

A Quick Cluster - 5 minutes

- 4 nodes
 - Raspberry Pi 3 Model B Plus Rev 1.3
 - Raspberry Pi 3 Model B Rev 1.2
 - Raspberry Pi 3 Model B Rev 1.2
 - Raspberry Pi 3 Model B Rev 1.2

```
$ k3sup install --ip 192.168.2.70 --user pi --context isis --local-path $HOME/.kube/config --k3s-channel latest
$ export KUBECONFIG=/Users/kat8172/.kube/config
```

```
$ kubectl get node -o wide
NAME    STATUS   ROLES   AGE    VERSION   INTERNAL-IP   EXTERNAL-IP   OS-IMAGE           KERNEL-VERSION   CONTAINER-RUNTIME
pitop   Ready    master   2m16s  v1.19.4+k3s1  192.168.2.70  <none>       Raspbian GNU/Linux 10 (buster)  5.4.72-v7+   containerd://1.4.1-k3s1
izzie1  Ready    <none>   2m3s  v1.18.12+k3s1  192.168.2.71  <none>       Raspbian GNU/Linux 10 (buster)  5.4.72-v7+   containerd://1.3.3-k3s2
izzie2  Ready    <none>   83s   v1.18.12+k3s1  192.168.2.72  <none>       Raspbian GNU/Linux 10 (buster)  5.4.72-v7+   containerd://1.3.3-k3s2
izzie3  Ready    <none>   51s   v1.18.12+k3s1  192.168.2.73  <none>       Raspbian GNU/Linux 10 (buster)  5.4.72-v7+   containerd://1.3.3-k3s2
```

16

curl -s0 https://packages.wazuh.com/4.12/wazuh-install.sh && sudo bash ./wazuh-install.sh -a

18

Break It – Learn It

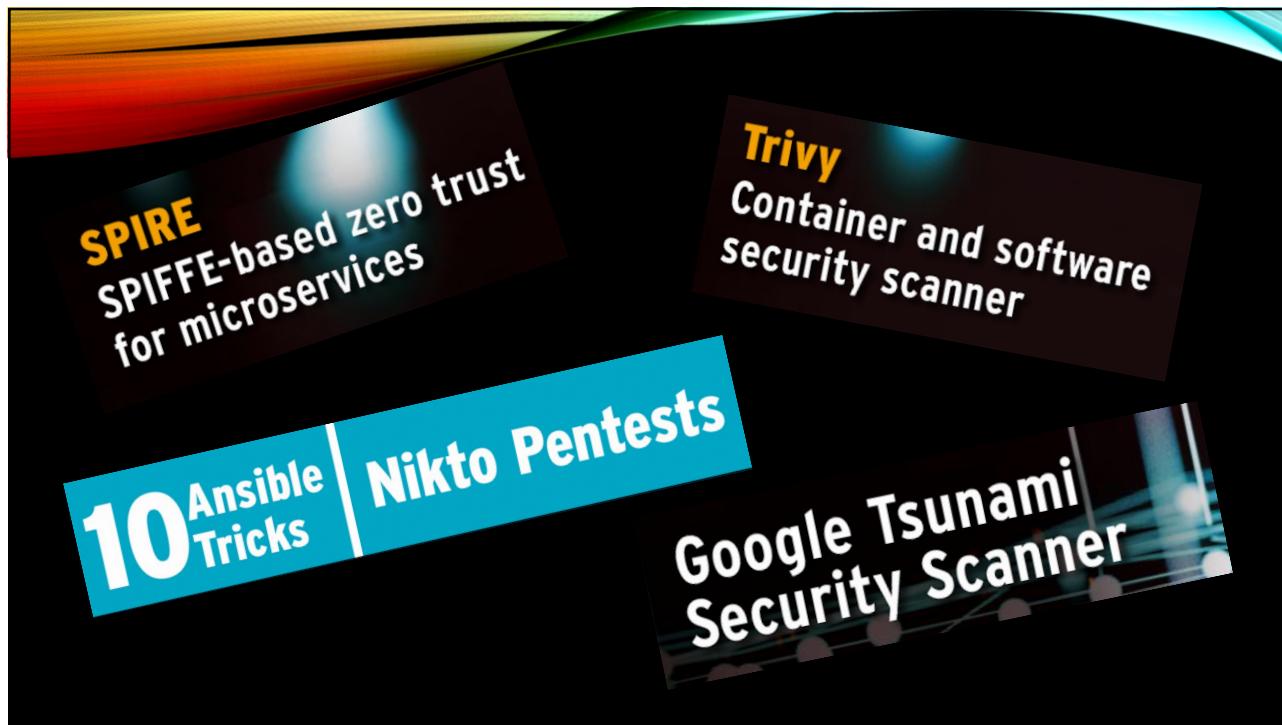
- VulnHub - www.vulnhub.com
- owasp.org/projects/
 - Learn secure coding - WebGoat owasp.org/www-project-webgoat
 - Practice modern AppSec attacks - Juice Shop owasp.org/www-project-juice-shop
 - Master recon & mapping - Amass owasp.org/www-project-amass
- SDR!! - github.com/luigifcruz/pisdr-image

19

The screenshot shows the VulnHub website interface. At the top, there's a navigation bar with the logo "VULN HUB" and links for "VIRTUAL MACHINES", "HELP", "RESOURCES", and "ABOUT". Below the navigation is a search bar with the placeholder "search by name or author" and filters for "SINGLE", "SERIES", "ALL", and "TIMELINE". The main content area displays three virtual machine cards:

- Matrix-Breakout: 2 Morpheus**: A card featuring a Matrix-themed image of Trinity. Description: "Welcome to the Box0Root CTF, Morphew! You play Trinity, trying to investigate a certain... Good luck! - @jaybeale from @inquisitor". Difficulty: Medium. Last updated: 11 Jul 2022 by Jay Beale.
- Web Machine: (N7)**: A card with a biohazard icon. Description: "about us". Difficulty: Medium. Last updated: 3 Nov 2021 by Duty Mastr.
- The Planets: Earth**: A card with a small icon. Description: "Bad Request". Difficulty: Easy. Last updated: 2 Nov 2021 by SirFlash.

20



21

Homelab AI Node – Project Overview

Project	Description	Core Hardware	Tools/Notes
SashaCam 5000	A next-gen AI surveillance node built on the Raspberry Pi AI Kit (M.2 HAT+ + Hailo-8 module).	Raspberry Pi 5, M.2 HAT+, Hailo-8, Pi Camera Module	YOLOv5 model, Hailo TFLite runner, image-to-alert pipeline

22

HONEYPOTS!

- OpenCanary -- opencanary.readthedocs.io/en/latest/
- ADHD – www.activecountermeasures.com/free-tools/adhd/
- Honey Badger -- github.com/adhdproject/honeybadger (GEO!)
- Community Honey Network --

 communityhoneynetwork.readthedocs.io/en/stable/
- Canarytokens -- canarytokens.org/generate
- T-pot -- github.com/dtag-dev-sec/tpotce
- Lots more -- github.com/paralax/awesome-honeypots

Personal Favorite – Honey “Data” in mysql/MSSql exposed to Internet

23

The screenshot displays the ADHD interface with several dropdown menus for selecting tokens:

- Top Left:** "Select your token" dropdown showing:
 - Windows folder**: Be notified when a Windows Folder is browsed in Windows Explorer.
 - Log4Shell**: Alert when a Log4j log line is vulnerable to CVE-2021-44228.
 - Fast redirect**: Alert when a URL is visited, User is redirected.
 - Slow redirect**: Alert when a URL is visited, User is redirected (More info is grabbed!).
 - Custom image web bug**: Alert when an image you uploaded is viewed.
 - Acrobat Reader PDF document**: Get alerted when a PDF document is opened in Acrobat Reader.
 - Custom exe / binary**: Fire an alert when an EXE or DLL is executed.
- Bottom Left:** "Select your token" dropdown showing:
 - Microsoft Excel document**: Get alerted when a document is opened in Microsoft Excel.
 - Kubeconfig token**: Alert when a Kubeconfig is used.
 - WireGuard VPN**: Alert when a WireGuard VPN client config is used.
 - Cloned website**: Trigger an alert when your website is cloned.
 - CSS cloned website**: Trigger an alert when your website is cloned (using CSS).
 - QR code**: Generate a QR code for physical tokens.
 - MySQL dump**: Get alerted when a MySQL dump is loaded.
- Top Right:** A list of tokens:
 - Microsoft SQL Server**: Get alerted when MS SQL Server databases are accessed.
 - SVN**: Alert when someone checks out an SVN repository.
 - Unique email address**: Alert when an email is sent to a unique address.
- Bottom Right:** A list of tokens:
 - Web bug / URL token**: Alert when a URL is visited.
 - DNS token**: Alert when a hostname is requested.
 - AWS keys**: Alert when AWS key is used.
 - Azure Login Certificate**: Azure Service Principal certificate that alerts when used to login with.
 - Azure Entra ID login**: Trigger an alert when your Azure Entra ID login is being phished.
 - Sensitive command token**: Alert when a suspicious Windows command is run.
 - Microsoft Word document**: Get alerted when a document is opened in Microsoft Word.

24

The screenshot shows the ADHD interface with the following components:

- Left Side:** A large red and orange abstract graphic with the text "ADHD" overlaid.
- Right Side:**
 - Logo:** ADHD ACTIVE DEFENSE HARBINGER DISTRIBUTION
 - Text:** ADHD Version: 4.0.0 | [GitHub Page](#) | [Project Page](#)
 - Section:** **ADHD**
 - List:**
 - **Credentials**
 - **Artillery**
 - Example 1: Running Artillery
 - Example 2: Triggering a Honeyport
 - Example 3: Adding a File to a Watched Directory
 - **Bear Trap**
 - Example 1: Basic Usage
 - **BeEF**
 - Example 1: Hooking a Web Browser
 - Example 2: Browser Based Exploitation With BeEF
 - **CanaryTokens**
 - Example 1: Creating Callbacks Using Local Canary Instance
 - Example 2: Creating Callbacks Using CanaryTokens.org
 - **Cowrie**
 - Example 1: Running Cowrie
 - Example 2: Cowrie In Action
 - Example 3: Viewing Cowrie's Logs

25

Picture Time!

- nextcloud.com – It just works!
- Tenable - [tenable.com/products/nessus/nessus-essentials](https://www.tenable.com/products/nessus/nessus-essentials)
- pwnagotchi.ai - Pi Zero! (dated, but still works!)
- homelabos.com – All-In-One
- Flare VM - github.com/mandiant/flare-vm
 - Windows malware-analysis & reverse-engineering VM
- CloudGoat - github.com/rhinosecuritylabs/cloudgoat
 - “vulnerable by design” cloud lab for IAM / S3 misconfig
- Kubernetes Goat- madhuakula.com/kubernetes-goat/docs
 - Kubernetes mis-configurations and attack/defence lab

26

Resume Sample

Technical Expertise

- I have cultivated a robust home security lab environment, enabling hands-on exploration and experimentation with cutting-edge cybersecurity tools and techniques. My experience includes thorough malware analysis, where I dissect samples to uncover behavioral patterns, isolate indicators of compromise (IOCs), and strategize effective mitigation tactics.
- I bring proficiency in penetration testing, adept at identifying and exploiting vulnerabilities across diverse systems, networks, and applications to fortify defenses proactively. Additionally, I excel in vulnerability research, consistently uncovering security flaws within software, firmware, and hardware components. My expertise extends to Linux hardening, implementing stringent measures to safeguard Linux-based environments from potential threats.
- Complementing these skills, I possess a strong foundation in incident response methodologies, network security protocols, and cryptographic algorithms, coupled with proficiency in scripting languages like Python and Bash for automation and custom tool development in cybersecurity operations.

27

Resume Sample 2

Technical Expertise

- **Home Security Lab:** Dedicated setup at home for hands-on research and testing of cybersecurity tools and techniques.
 - **Malware Analysis:** Proficient in analyzing malware samples to understand behavior, identify indicators of compromise (IOCs), and develop mitigation strategies.
 - **Penetration Testing:** Experience in conducting penetration tests to identify and exploit vulnerabilities in systems, networks, and applications.
 - **Vulnerability Research:** Skilled in researching and discovering security vulnerabilities in software, firmware, and hardware components.
 - **Linux Hardening:** Expertise in hardening Linux-based systems to enhance security posture and mitigate potential threats.
- **Additional Skills:** Familiarity with incident response procedures, network security protocols, and cryptographic algorithms. Proficient in scripting languages such as Python and Bash for automation and tool development in cybersecurity operations.

28

Resume Sample 3

Technical Expertise

- Home Security Lab:** Dedicated setup for hands-on security research, network segmentation, and threat detection.
- **Intrusion Detection & Prevention:** Configured **Suricata** to monitor and analyze network traffic, identifying potential threats and anomalies in real time.
 - **Firewall & Network Segmentation:** Deployed **OPNsense** with VLANs to **isolate IoT devices**, reducing attack surface and mitigating lateral movement risks.
 - **Network Traffic Analysis:** Developed rules and alerting mechanisms to **detect suspicious activity from IoT devices**, enhancing network visibility.
 - **Threat Hunting & Incident Response:** Used Suricata logs to investigate security events, refine detection rules, and **improve automated threat response strategies**.
 - **Security Automation & Scripting:** Utilized **Python and Bash** to automate log analysis, rule updates, and alert tuning for optimized security operations.

29

Resume Sample 4

Technical Expertise

- **AI-Driven Security Lab:** Built a fully operational home lab integrating AI tools with traditional security infrastructure to enhance threat detection, analysis, and response.
- **AI Integration & SOC Automation:** Deployed LLaMA 3 locally to summarize Suricata and Wazuh logs, enabling natural-language incident reports and reducing analyst alert fatigue.
- **Edge AI Inference:** Implemented Raspberry Pi AI Kit (Hailo-8) to run YOLOv5 models for real-time object detection and anomaly flagging in surveillance environments.
- **Threat Detection & Log Correlation:** Combined Suricata, Zeek, and Wazuh to monitor, correlate, and triage alerts from multiple honeypots and segmented network zones.
- **SOC Tools Deployment:** Configured alert pipelines, dashboards, and alert tuning using open-source tools like Wazuh, Elastic, and custom scripts.
- **Security AI Prompt Engineering:** Developed effective prompts and automation scripts to guide local LLMs in daily summarization and pattern recognition of security data.
- **Automation & Custom Tooling:** Leveraged Python and Bash to automate data ingestion, enrichment, and AI-driven response recommendations.

30

the forgotten training/Learning

"Learning from a great teacher is discovery, not studying."

- antisyphontraining.com
 - Ranging from Noobs to most Senior
 - Free and Pay-what-you-can
- tcm-sec.com
 - Beginner to advanced and all kinds of discounts throughout the year
- tryhackme.com & academy.hackthebox.com
 - Gamified trainings – I do both myself!

31

KEY TAKEAWAYS

- It's Playtime!
 - The beauty of virtualization
 - Don't forget about containers/proxmox
- There is no right or wrong
- Start small / build on it
 - Break it – build it – break it again
- You can get sucked in
 - Make a plan!



32

Kat Fitzgerald

github.com/rnbwkat/presents
 rnbwkat@infosec.exchange
 rnbwkat.bsky.social
 YT/@rnbwkatandtequila

evilkat@rnbwmail.com

sashatheflamingo.xyz

Thank You!

infosec.exchange/@sashatheflamingo
@sashatheflamingo.bsky.social



33