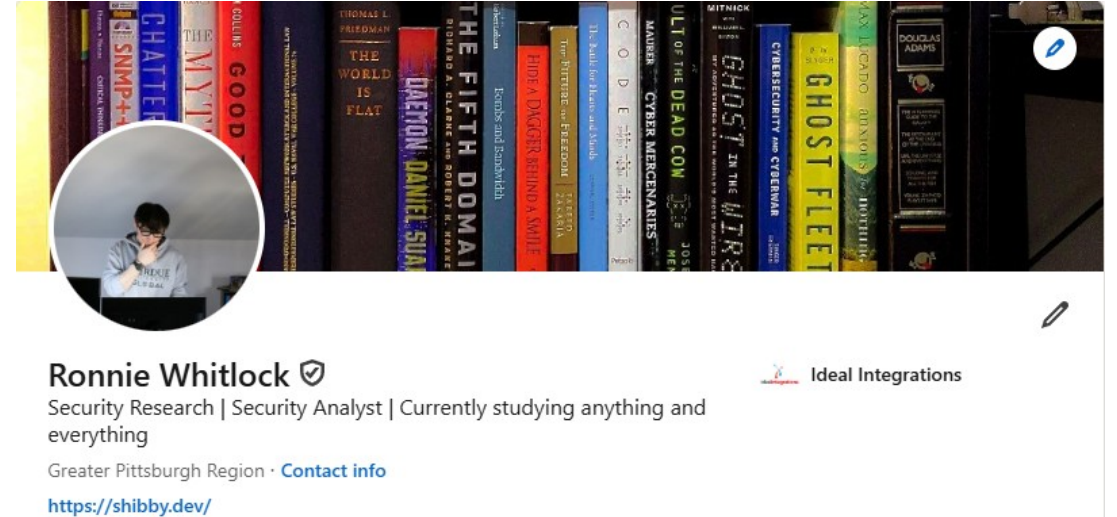


FOSS CTI Guide to Security Operations

Free and Open Source Software guide to Cyber Threat
Intelligence for Security Operations

Whoami

- Security Analyst for Blue Bastion a division of Ideal Integrations
- MDR, Vulnerability Management
- Focus areas
 - Detection and Analysis
 - Threat Intelligence
 - Vulnerability Research
- Networking/IT Admin background
- OAC Committee Member
- I want to see this industry thrive
- Book worm – Business strategy, leadership and tech



What this talk is

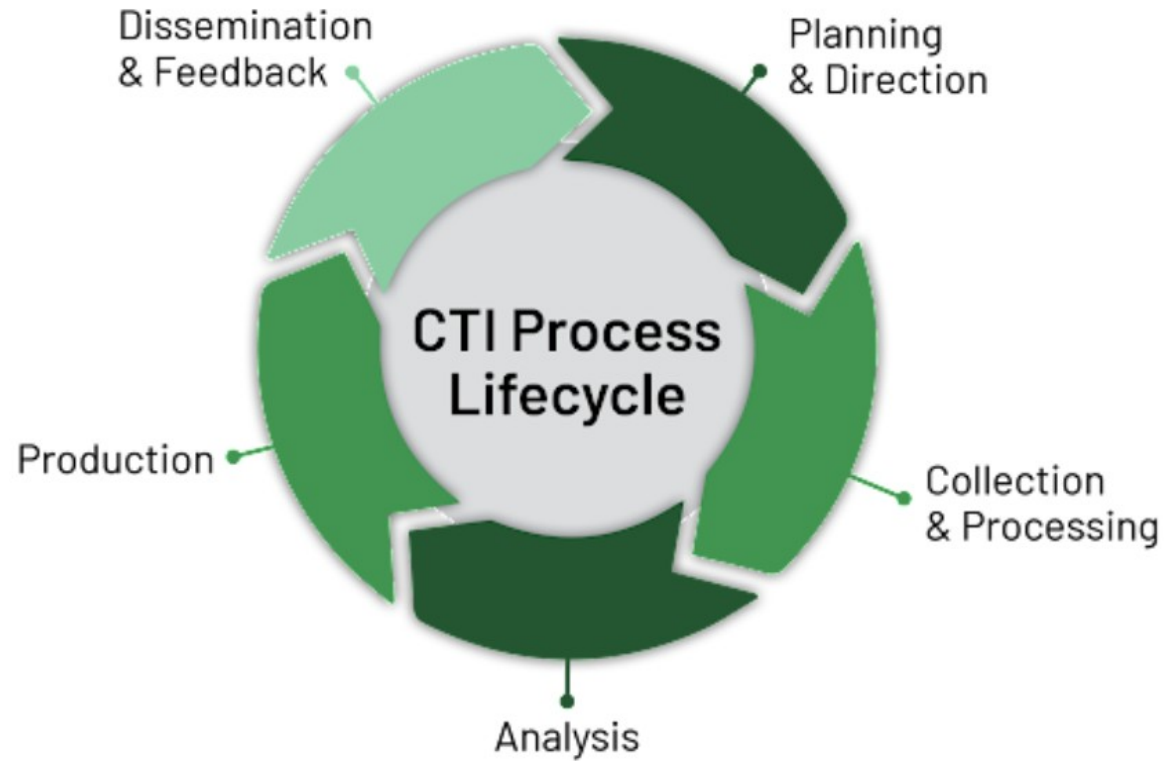
- Value of CTI in SOC Operations
- Life Cycle
- Classifying
- Stack – Surface level

CTI Value

- Most offensive thing about defense
- Proactive vs Reactive
- Investigation Enrichment



Lifecycle



Types and the audience

- Strategic – Risk based (shareholders, C-Level)
- Tactical – Immediate (Analyst, Incident Responder)
- Operational – Persistent Protection (Detection Engineers, SOC Engineers)

The Stack

Cert.pl Toolkit – MWDB, Karton, Drakvuf

MISP/OpenCTI, Synapse

Honeypotting

Feeds – VirusTotal, Greynoise, Valadin, etc

Dalton



Cert.pl

- Cert Polska is a team within the NASK National Research Institute
- Research and develop in areas of cybersecurity, biometrics, ICT, ICS, IoT, AI, Big Data technologies, social networks
- <https://github.com/CERT-Polska>
- Other tools – Artemis vulnerability scanner

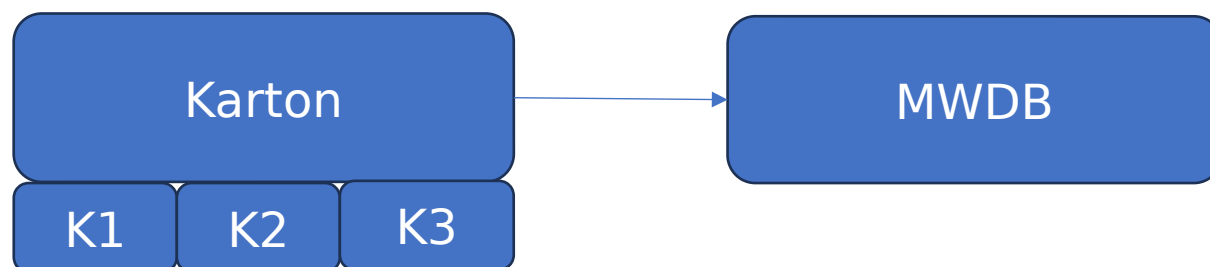
Karton Framework

- Queue based pipeline to database
- Based on Redis and S3-compatible object storage
- Microservice
- Classifier, archive extractor, config extractor, **MWDB Reporter**, yaramatcher, decode ascii, **Drakvuf Integration**



MWDB

- Malware Database, central component for binaries
- Aggregates various feeds and collections
- Integrates with MalwareBazaar
- Focuses on artifacts and analysis of samples
- Stores metadata such as SHA, md5, and ssdeep hashes, associated APTs
- Rest API or python integration called mwdblib



Drakvuf

- Built off of IntelVT-x and EPT using Xen
- Based off of Karton for pipeline
- Dependencies: Qemu for machine emulation, genisio for file information, bridgutils and dnsmasq for networking, and libmagic1 for file classification
- LibVMI for virtual machine introspection, monitor details and changes to virtual machine
- Sends back to MWDB to enrich binarys attributes

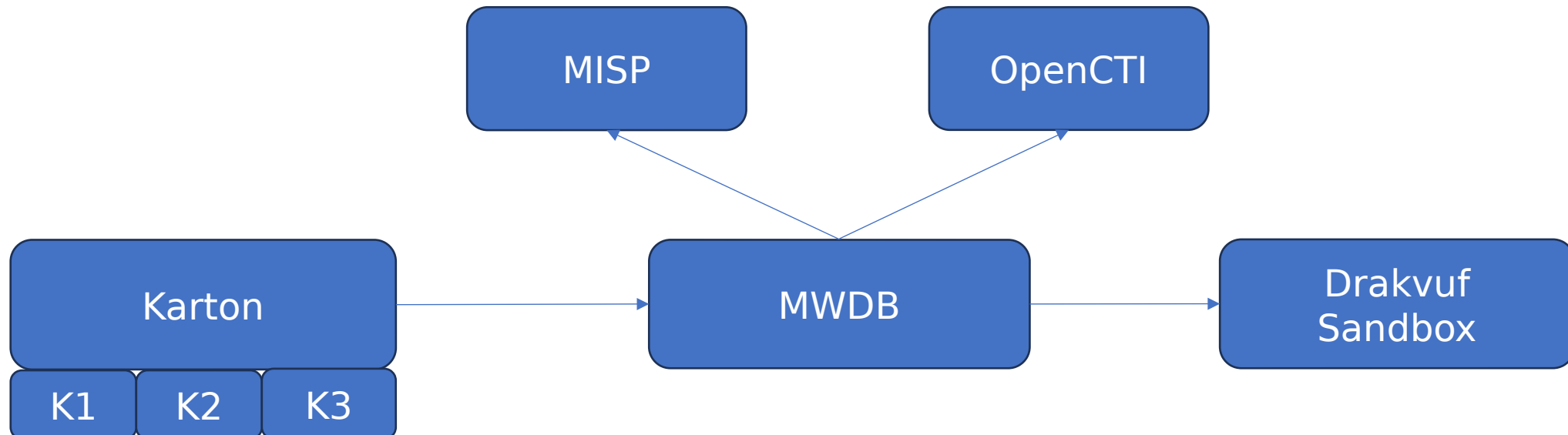


Share – MISP/OpenCTI

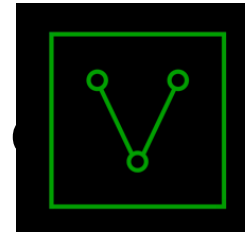


OPENCTI

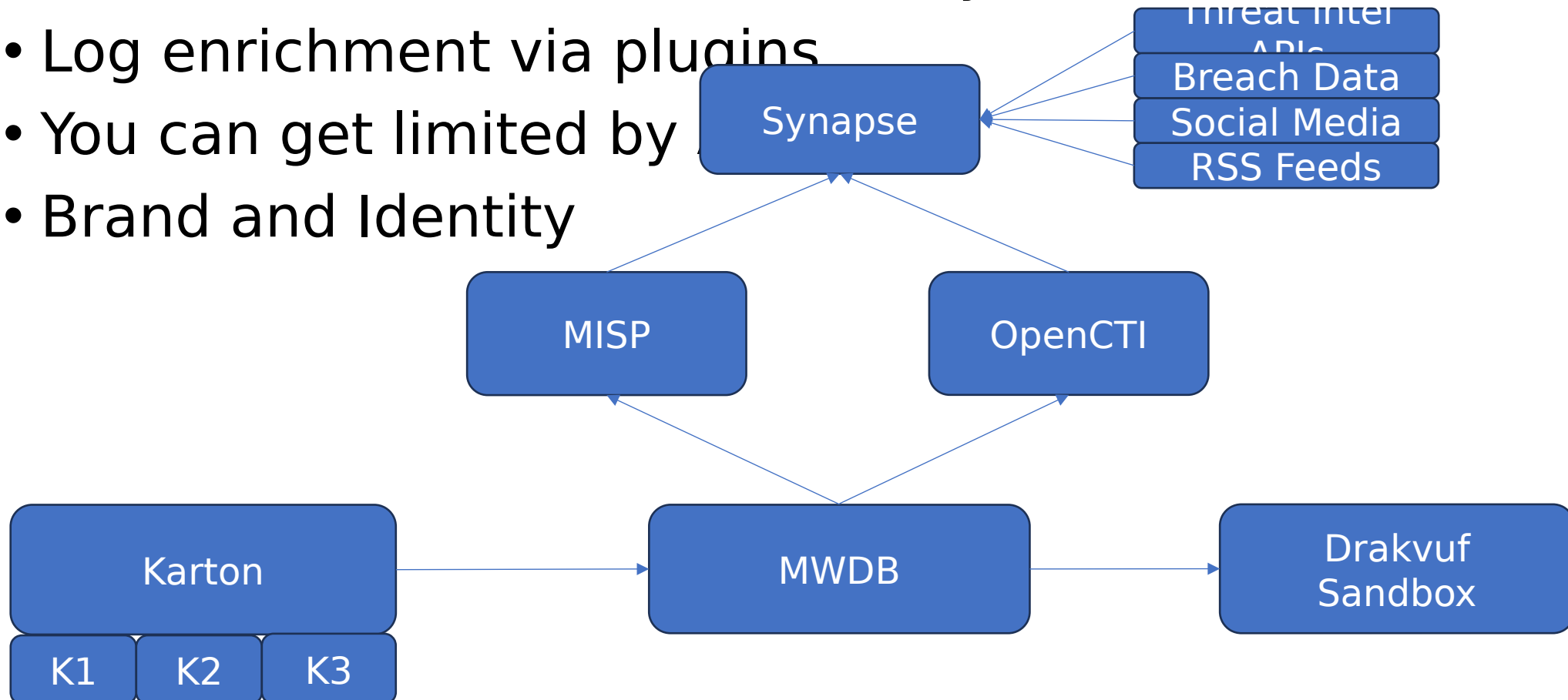
- Misp 2011 (More developed)
- OpenCTI 2018 (Easier more modern UI)
- In this stack this is just for sharing and unification of the binaries data



The Vertex Project Synapse



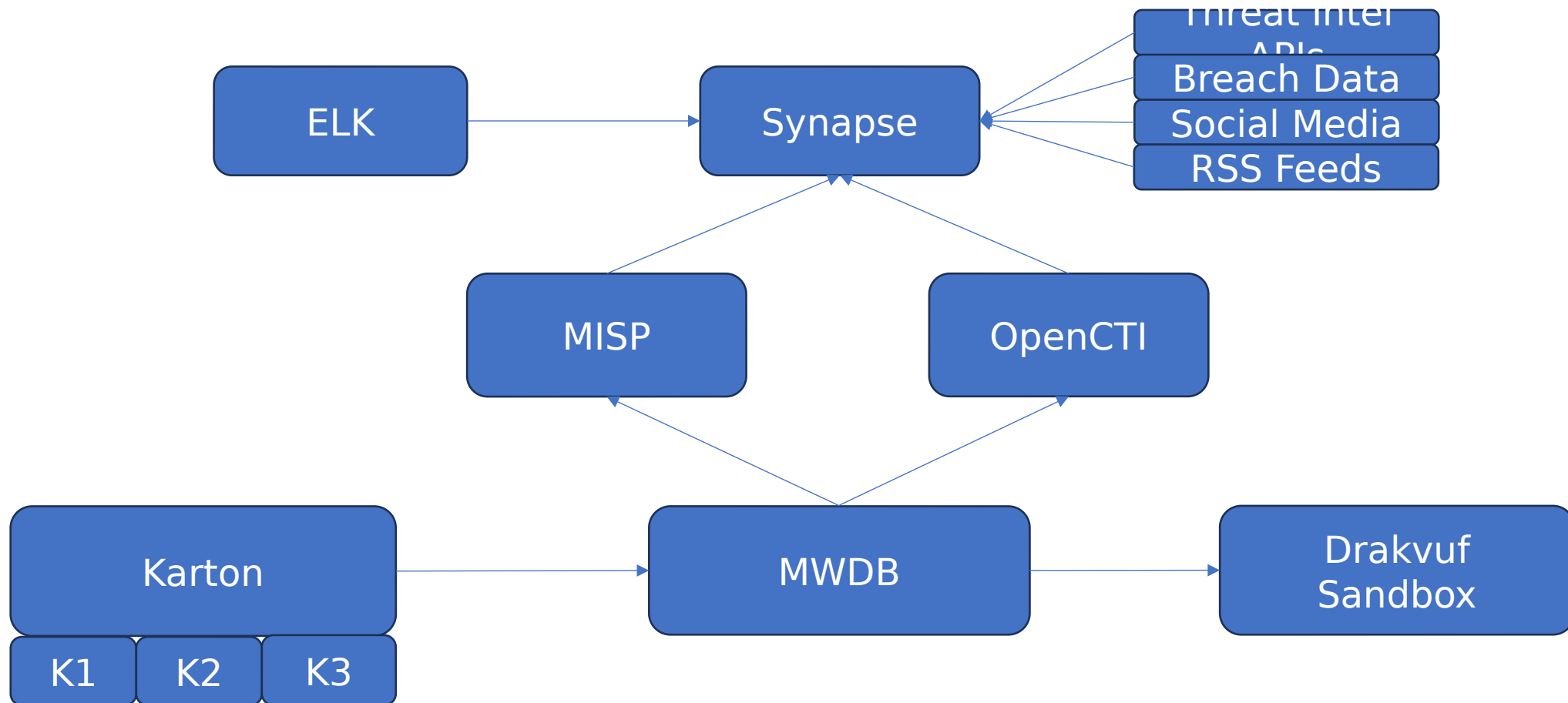
- Unification of ALL data and analysis
- Log enrichment via plugins
- You can get limited by
- Brand and Identity



Honey potting - tp



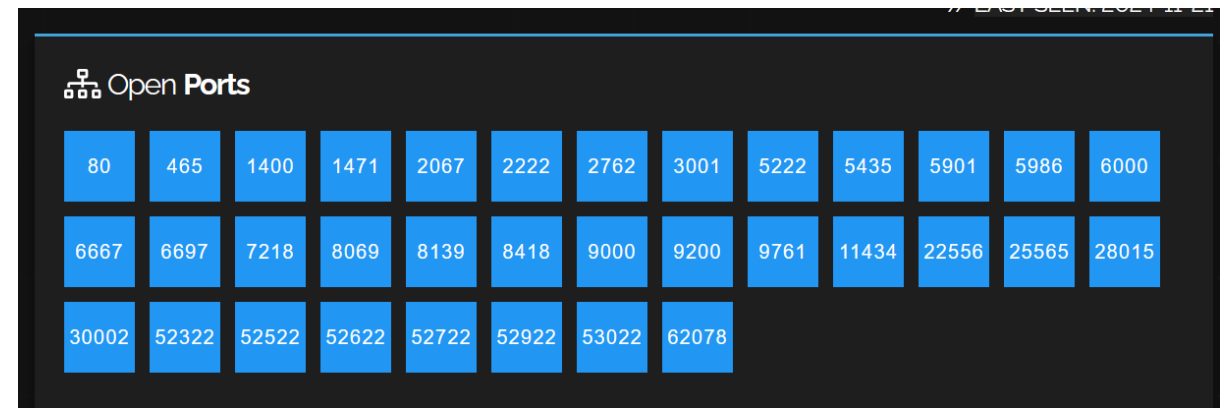
- PCAP Collection



Tpot



- 23 Honeypots
- Maintained by Telekom Deutschland
- <https://github.com/telekom-security/tpotce>
- adbhoney, beelzebub, ciscoasa, citrixhoneypot, conpot, cowrie, ddospot, dicompot, dionaea, elasticpot, endlessh, galah, go-pot, glutton, h0neytr4p, hellpot, heralding, honeyaml, honeypots, honeytrap, ipphoney, log4pot, mailoney, medpot, miniprint, redishhoneypot, sentrypeer, snare, tanner, wordpot

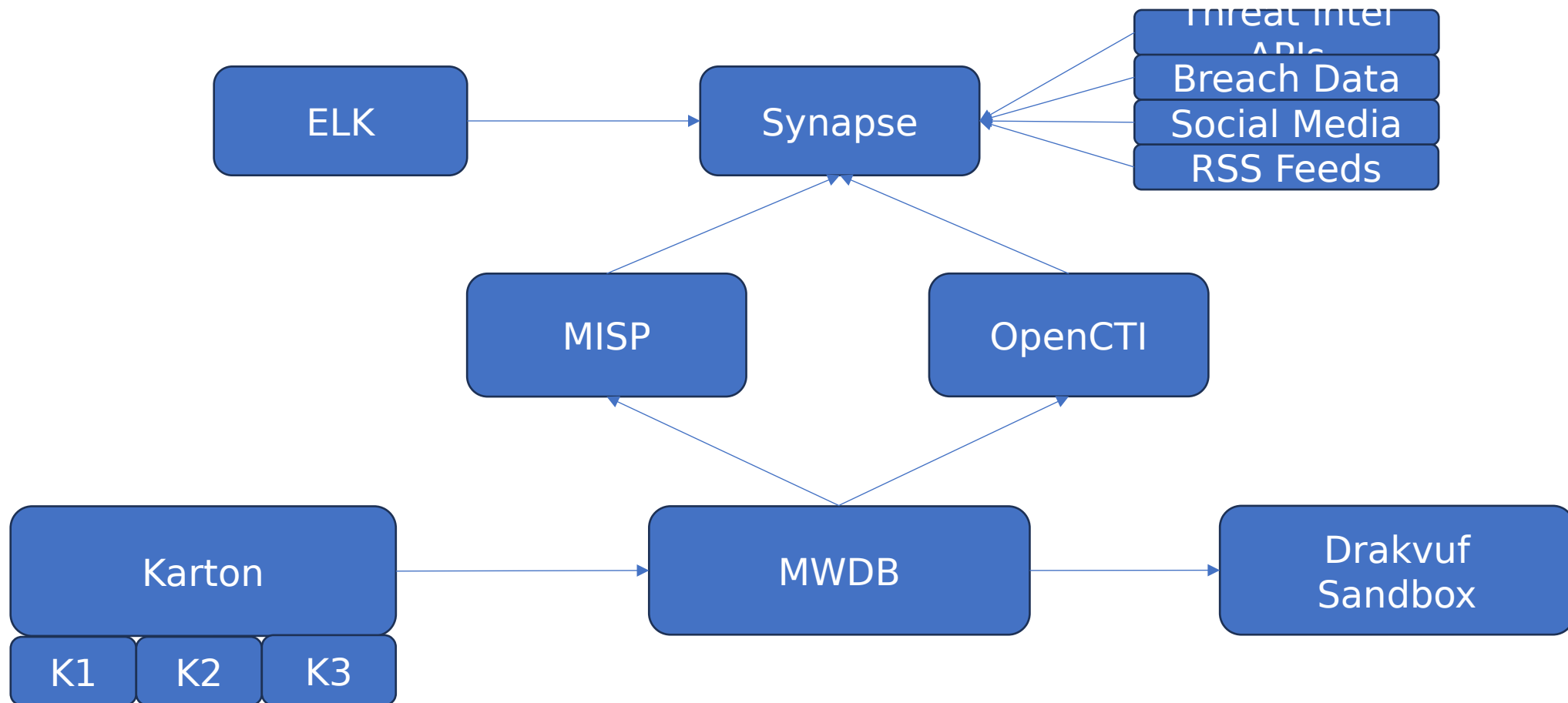


80	465	1400	1471	2067	2222	2762	3001	5222	5435	5901	5986	6000
6667	6697	7218	8069	8139	8418	9000	9200	9761	11434	22556	25565	28015
30002	52322	52522	52622	52722	52922	53022	62078					

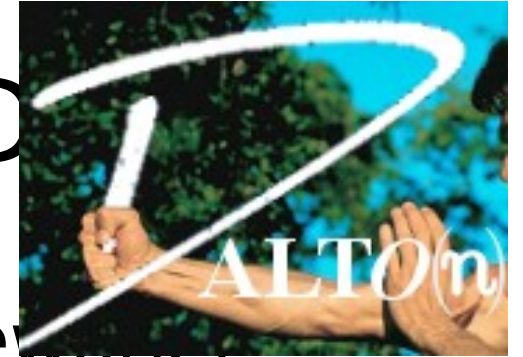
Honey potting - tp



- PCAP Collection

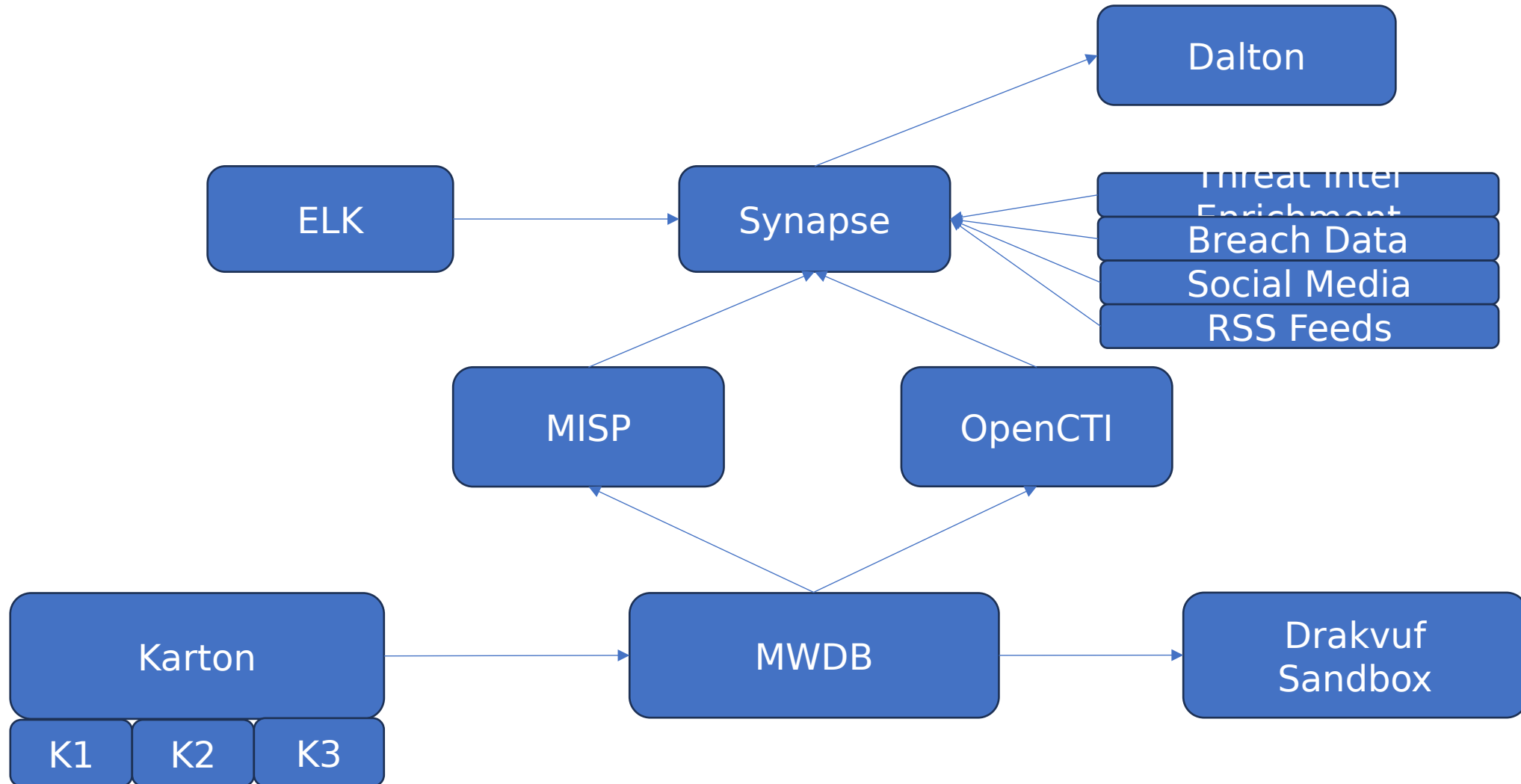


Detection Engineering using Dalton

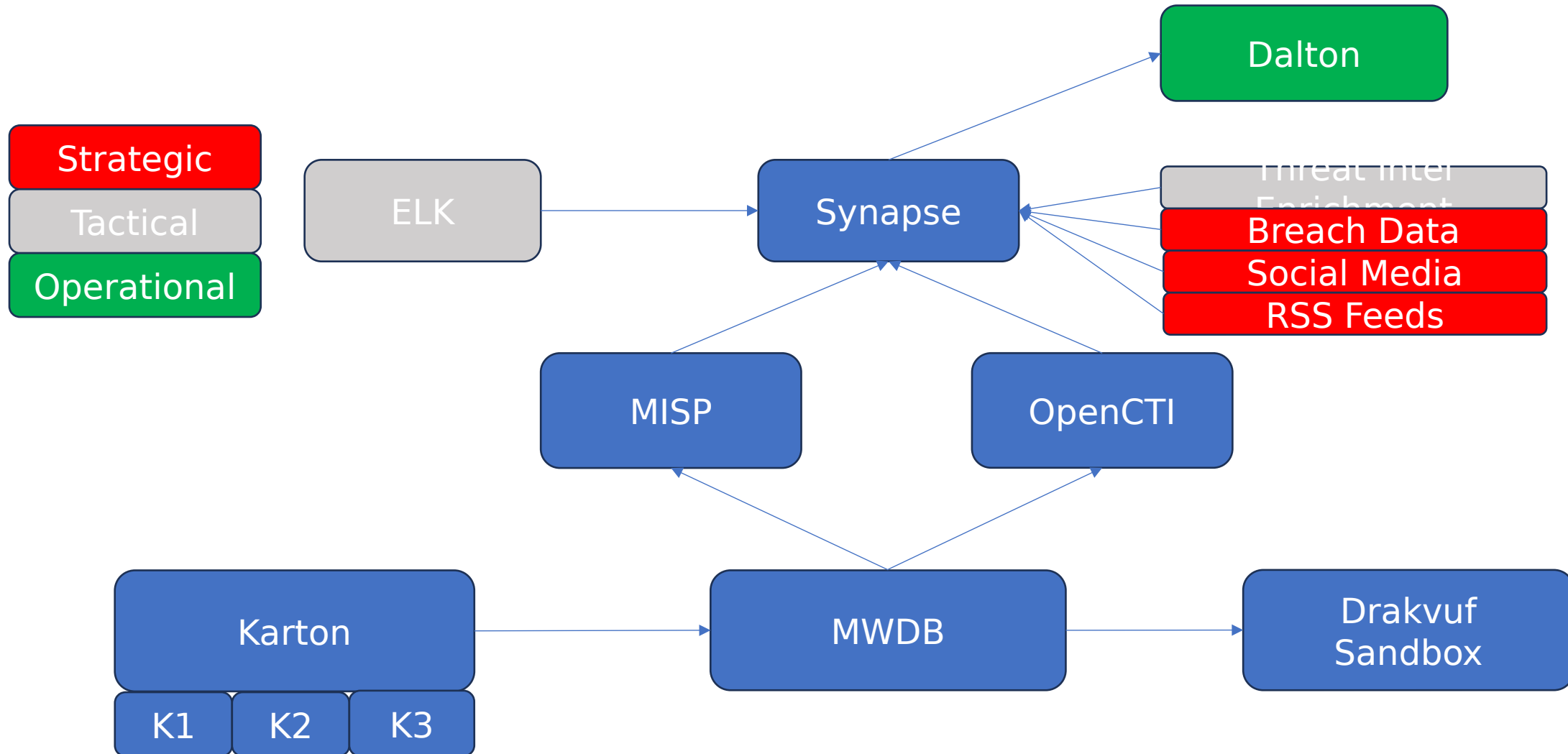


- Developed and made open sourced by secureworks
- Dalton is a tool to test your pcaps against your IDS rules
- Zeek, suricata, snort
- Can be deployed via docker
- <https://github.com/secureworks/dalton>

Dalton in the stack



What do we have now?

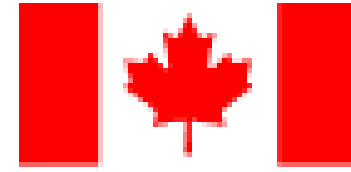


What data do we have

- External/Internal PCAP
- Malware samples and IOCs
- RSS Feeds and reports
- Social media data



Honorable Mentions



- Assembly Line - <https://github.com/CybercentreCanada/assemblyline>
- Similar to Karton and mwdb
- Automated
- Docker/Kubernetes
- File risk scoring
- Sent to other security tools

Honorable Mentions



- Cuckoo sandbox - <https://github.com/cuckoosandbox/cuckoo>
- Compared to drakvuf
- Agent based sandboxing
- Can emulate mac, linux, and android



Honorable Mentions

- IntelOwl- <https://intelowlproject.github.io/>
- Compared to MISP/OpenCTI and Synapse
- Analysis

Honorable Mentions



- The HoneyNet Project - <https://www.honeynet.org/projects/>
- non profit
- Google Summer of Code – mentors students to become open-sourced contributors
- Tpot, intelowl

Honorable Mentions Repos

- Awesome threat intel - <https://github.com/hslatman/awesome-threat-intelligence>
- Open source cti tools - <https://github.com/BushidoUK/Open-source-tools-for-CTI>
- Threat Actor TTPs - <https://github.com/crocodyli/ThreatActors-TTPs>
- Deepdarkcti - <https://github.com/fastfire/deepdarkCTI>

Take Aways

- Methods of CTI Collection
- Types of CTI and its value to Security Operations and business enablement
- Other toolsets
- Cater it to your environment or clients. Is this something you want to add to a msp stack for clients to benefit?

Socials

- LinkedIn – Ronnie Whitlock
- Twitter – Ronniyobp
- Bluesky – shibby.dev

Questions?

