Say hello
Introduce trip briefly

Why “Deceptive Defences”

Participated in a number of risk assessments where honeypots have been proposed and rejected
Systems that are hard to monitor (SIEM, NIDS)
Legacy networks that you can hardly touch
Risk Assessment Story – “You just don’t know what to do”

Goal:

By the end of today, you'll understand how to deploy effective honeypots in your network with tools that can be set up in under an hour.

Agenda


Brief History


Purpose


Types

Use Cases


Examples


Global Use


How?

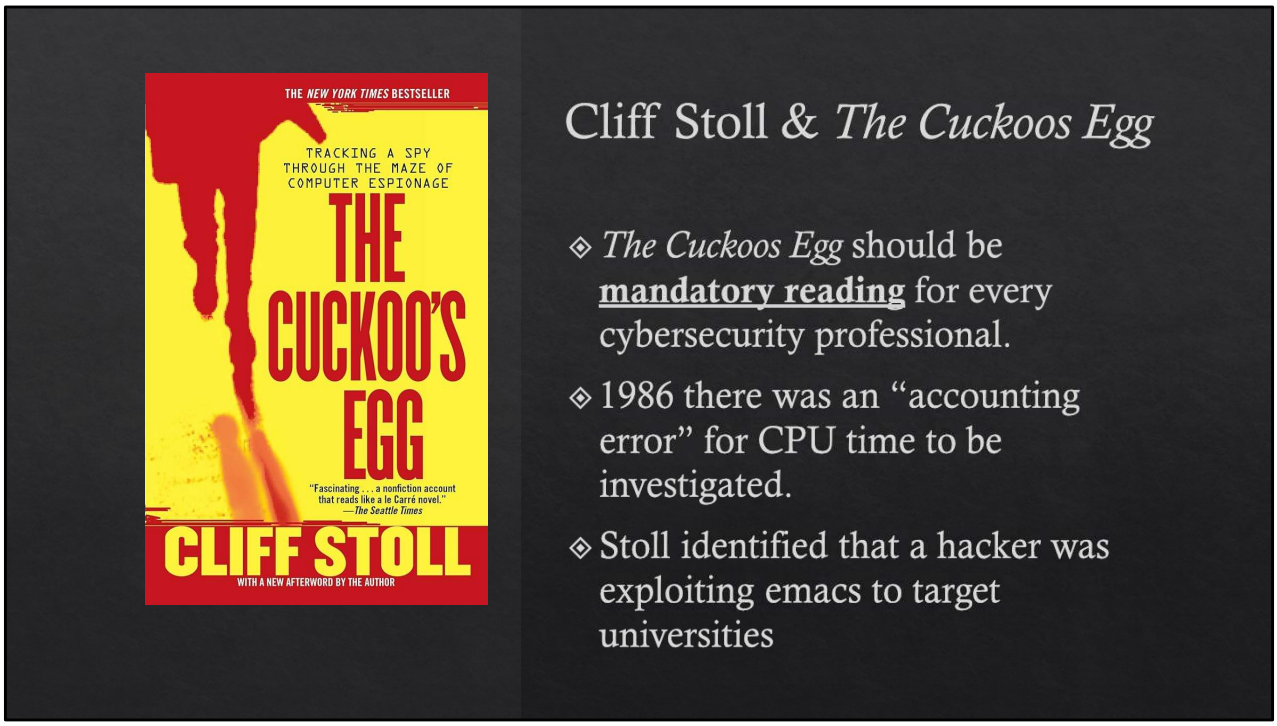
Introduction to Honeypots

- Ancient form of espionage
  - Kautilya's *Artahastra*
  - Sir Francis counter-espionage vs Catholics
  - Napoleonic War fake mail deaddrops
- Ultimately originates with HUMINT gathering

Plant spies in enemy ranks or lure enemies into false confidence

Sir Francis Walsingham (Elizabeth I spymaster) setting up fake channels for Catholic plotters (Babington Plot)

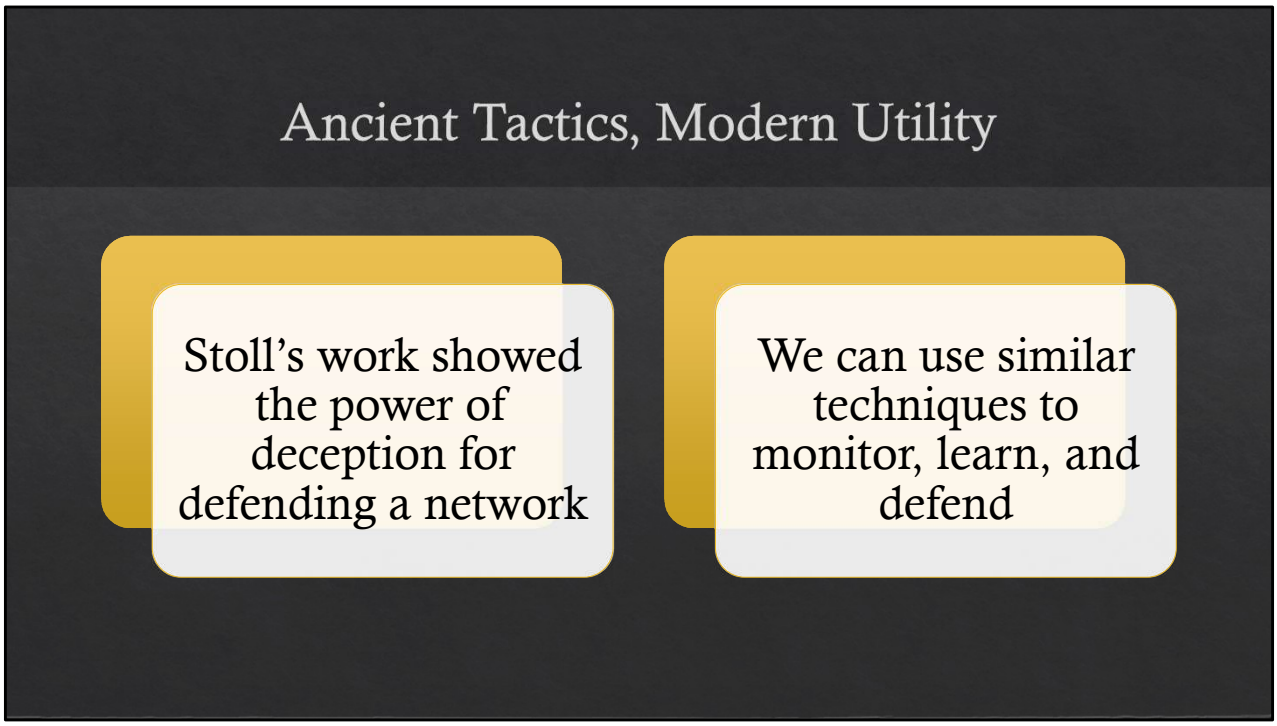
British/Allied forces setting up Fake Mail drops during the Napoleonic War to track movements of spies



Cuckoos egg is a great book and one that I recommend every time I do an open career day for students

Stoll was a physicist on loan to be a sysadmin
Accounting error on one of their machines – each department had to pay for CPU time, clock time
After a long investigation he identified that a hacker was accessing their department from overseas due to a vulnerability in emacs

It was a long process to track the hacker, as they were dialing in from University of Bremen (and also their own home in Bremen).
Delay was with the German Post Office who ran all internet lines for (Western) Germany
Needed to keep the hacker on the line long enough for workers to track which phone line was being used.
Stoll created a "honeypot" with fake defence documents so the hacker was interested enough to stick around



Like Sir Francis' traps for catholic spies, Stoll's honeypot gave false info to the attacker
This deception prevented the attacker from strolling elsewhere through the network
Because of this honeypot the attacker was able to be tracked and stopped
While it's unlikely we will be able to "track" or arrest hackers we will see, we can still deceive them
By deceiving them we can prevent them from potentially attacking assets we care about long enough for us to track them (internally)

This is all part of your ACTIVE DEFENCE

Agenda


Brief History


Purpose


Types

Use Cases


Examples


Global Use


How?

Honeypots as an Information Gathering Tool

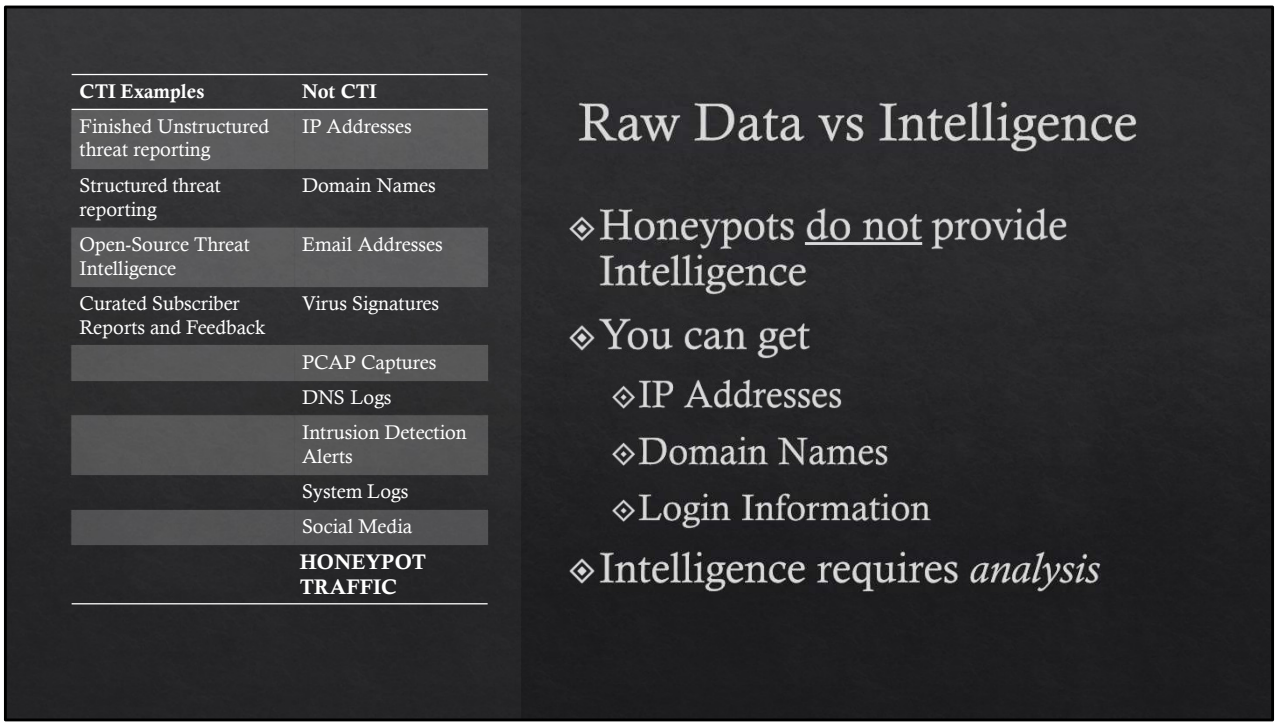
External, vulnerable system that logs attack information maps

Provide lots (*lots!*) of information about attacks

How much of that is useful?

Typical honeypot use that I think post people expect

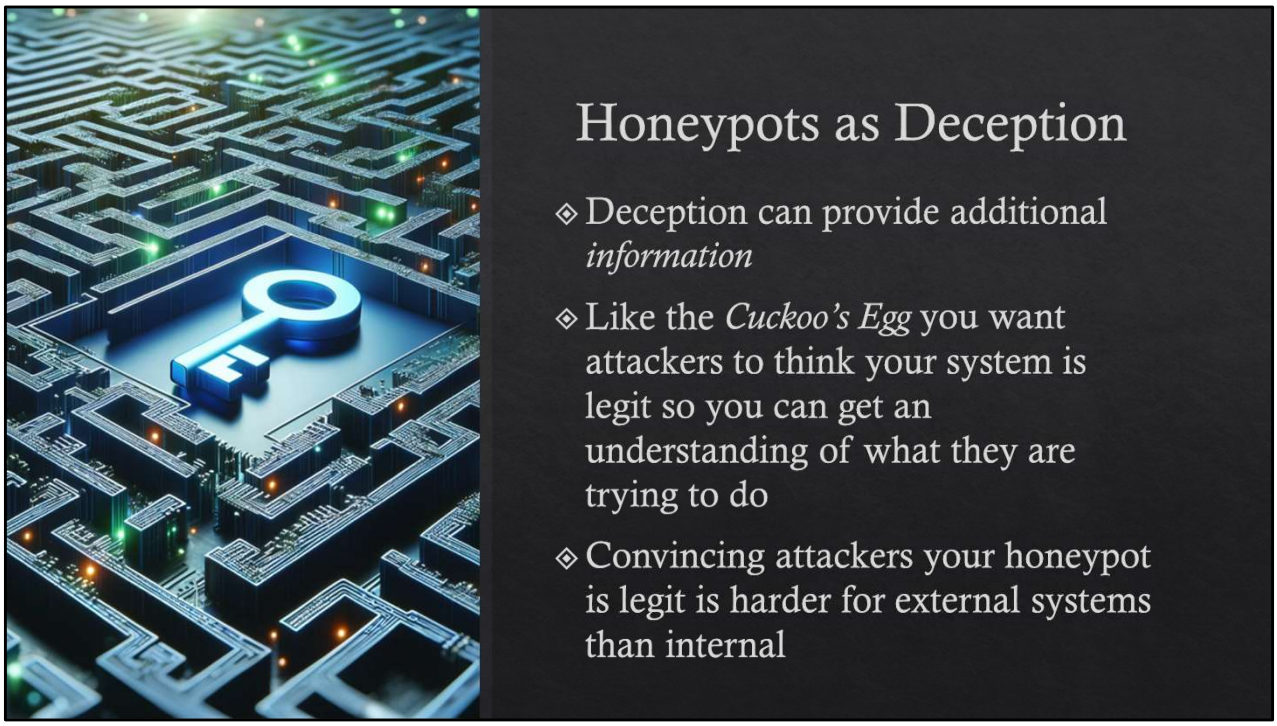
Norse attack map (lol)



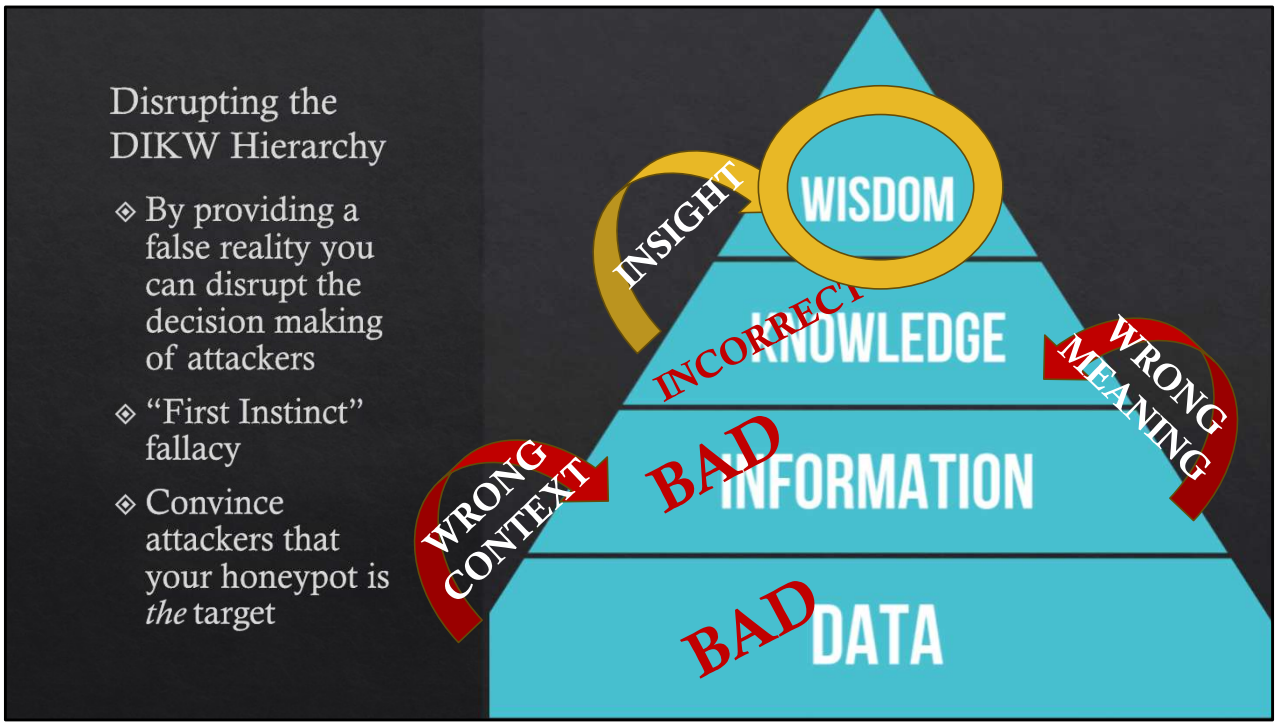
Honeypots will not give you INTELLIGENCE

Intelligence requires ANALYSIS

We will not be talking about data analysis



The DECEPTION of honeypots is convincing attackers your honeypot is legit, valid target
We think about swiss cheese – they might already be in the network through another hole
We collect that information and can act on it as part of our ACTIVE DEFENCE



"First Instinct" fallacy is that once presented with data, and you make your logical decision, you fit the narrative of your data to match

Structured Analytical Techniques help reduce bias, promote logical reasoning to prevent that. If we assume our attacker is trained they might know to do this.

We interfere with the DIKW hierarchy to promote bad data and incorrect context, from which attackers can infer the wrong meaning (knowledge) and apply their insight on it (TTPs) to generate bad wisdom

Potential Early Threat Detection
Information Gathering on Attacker TTPs
Misdirection
Strengthen security controls where monitoring might not be possible

Quick few text slides to make sure we're on the same page with different systems

Low-Interaction: Quick and Lightweight

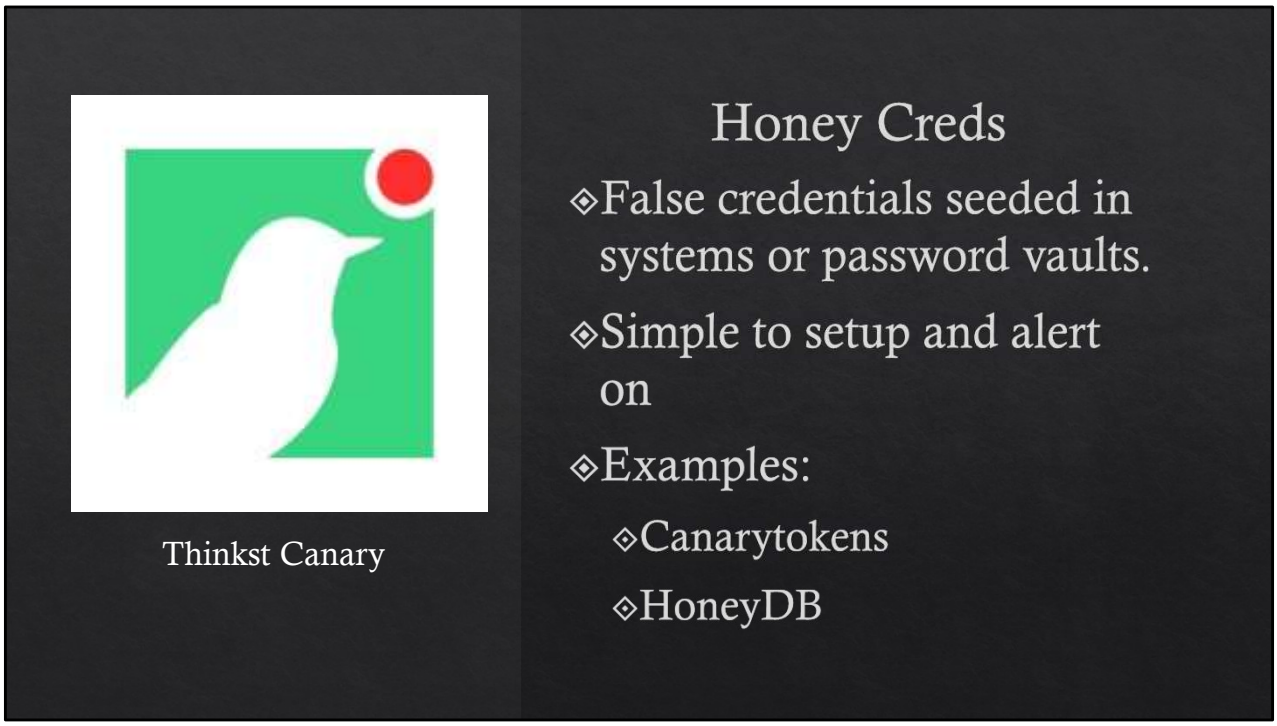
- Simulate limited services – SSH, FTP
- Detect and log interactions with minimal resources
- Example OS Tools:
  - Dionaea: Emulates vulnerable services to capture service requests
  - Cowrie: SSH/Telnet honeypot that records interactions

High-Interaction: In-Depth Engagement

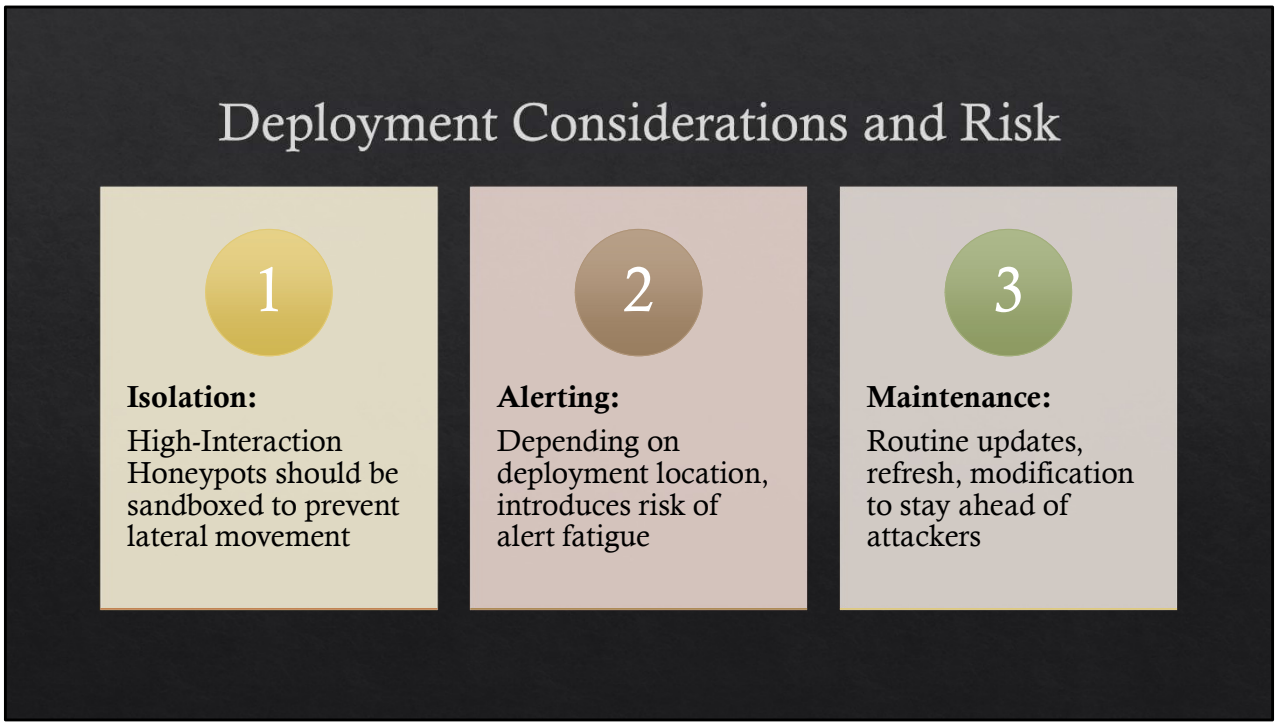
- Emulates full systems
- Gathers extensive data but requires extensive analysis / monitoring
- Example OS Tools:
  - HIHAT – PHP Web Service Emulator
  - Lyrebird – exposes real vulnerable applications but MITM all traffic
  - Honeyfs – File System

This requires *ANALYSIS*.

This requires extensive team investment



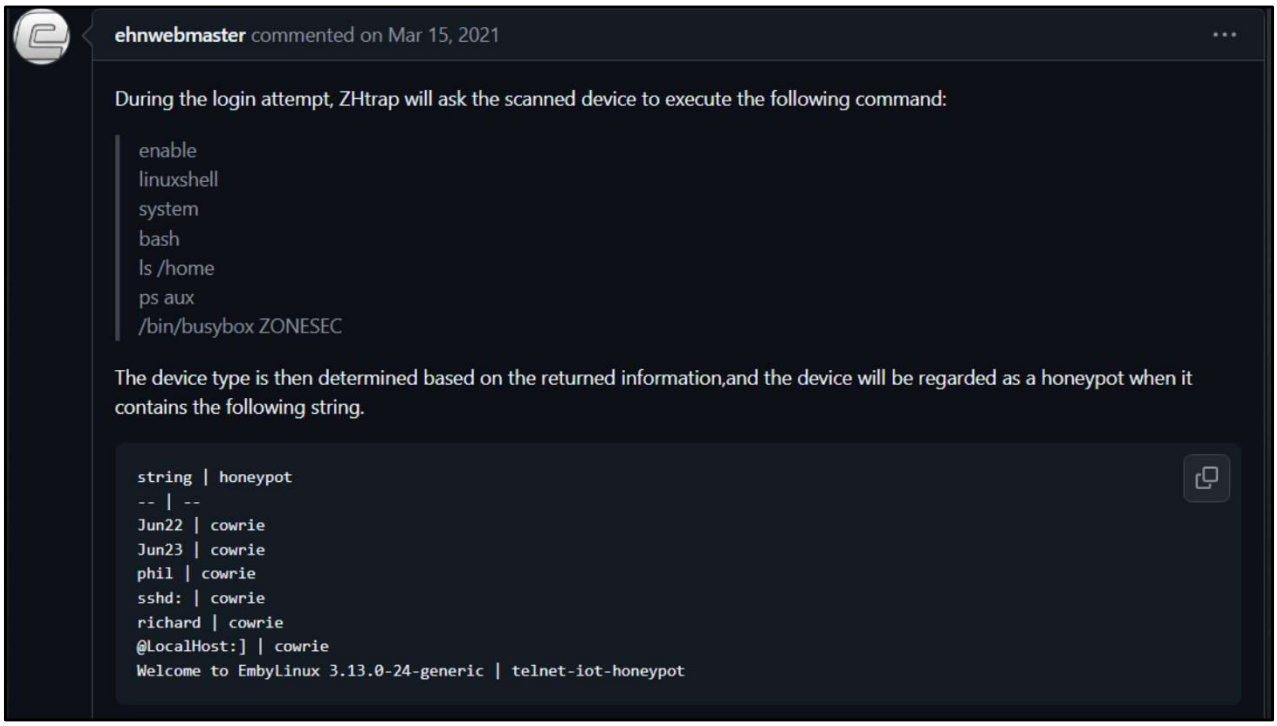
You can do this in ActiveDirectory or with your own DNS logging or Thinkst Canary is a very popular product in this area for mass, cheap, deployment



H-I Honeypots can essentially be considered full systems. Think back to Stoll – full system of data.

Alerting – can be difficult if you don't manage alerting strategy well. This should be considered as a whole of operations approach. Look at Palantir's Alerting Detection Strategy for examples.

Maintenance – honeypots, especially external, will require upgrades to defeat mass scanners if you're hunting for information. Internal, not so much, but still a potential risk to consider.



ehnwebmaster commented on Mar 15, 2021

During the login attempt, ZHtrap will ask the scanned device to execute the following command:

> enable
> linuxshell
> system
> bash
> ls /home
> ps aux
> /bin/busybox ZONESEC

The device type is then determined based on the returned information,and the device will be regarded as a honeypot when it contains the following string.

string	honeypot
Jun22	cowrie
Jun23	cowrie
phil	cowrie
sshd:	cowrie
richard	cowrie
@LocalHost:]	cowrie
Welcome to EmbyLinux 3.13.0-24-generic	telnet-iot-honeypot

Cowrie github issue from 2021

ZHTrap botnet

Log into vulnerable systems then check to see if it's sandboxed. If you want your systems to stay covert and collect information (drop malware) then you'll need to avoid this detection.

Selecting the Right Honeypot for your Needs

Honeypot	Purpose	Potential Location	Data
Low-Interaction	Quick Detection, minimal monitoring	Perimeter / DMZ / high traffic areas	Ips, basic threat information
High-Interaction	Deeper engagement, assessment of TTPs	Sensitive areas (lateral movement)	Detailed command history, dropped files
HoneyCreds	Simple monitoring/alerting	Scattered liberally	Access attempts with context

Agenda


Brief History


Purpose


Types

Use Cases

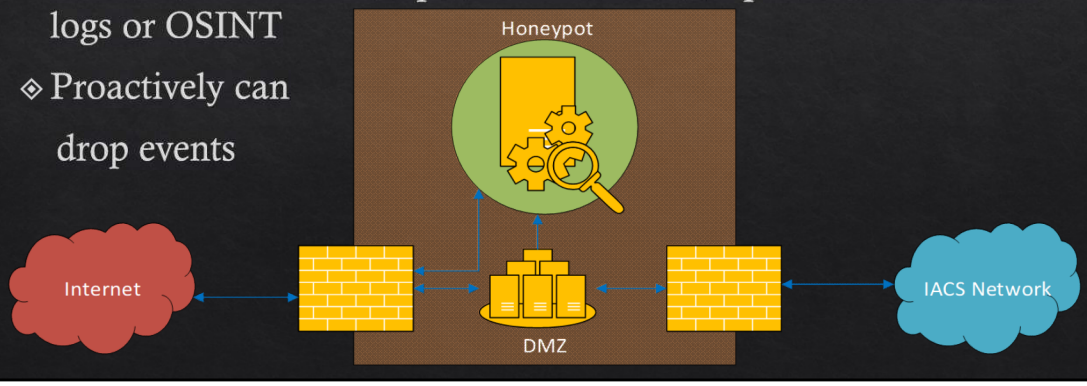

Examples


Global Use


How?

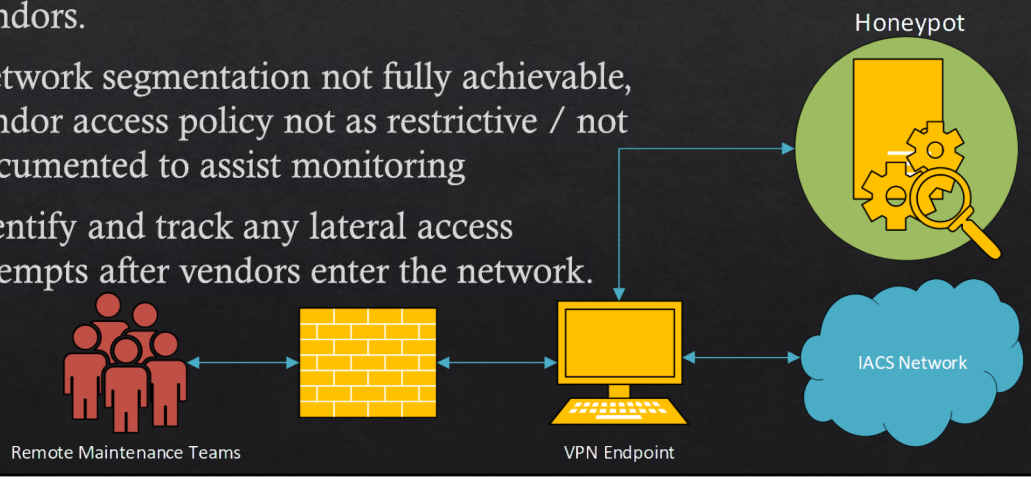
Detecting Reconnaissance and Port Scanning

- Perimeter zones to attract reconnaissance / port scanning (most likely automated)
- Dedicated information pool that can be compared with firewall logs or OSINT
- Proactively can drop events



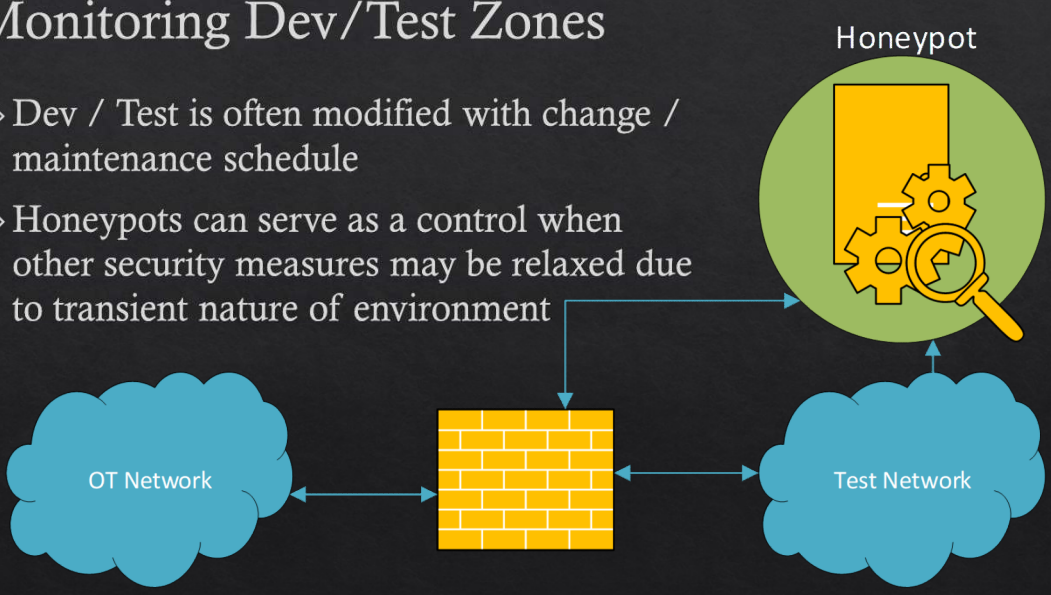
Monitoring Untrusted Vendors

- Remote Access jump-zone for external vendors.
- Network segmentation not fully achievable, vendor access policy not as restrictive / not documented to assist monitoring
- Identify and track any lateral access attempts after vendors enter the network.



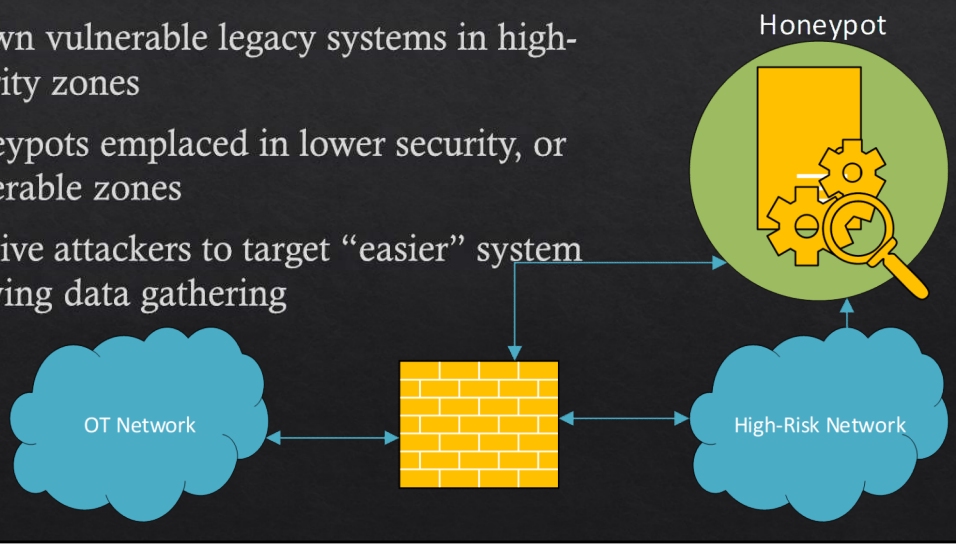
Monitoring Dev/Test Zones

- Dev / Test is often modified with change / maintenance schedule
- Honeypots can serve as a control when other security measures may be relaxed due to transient nature of environment



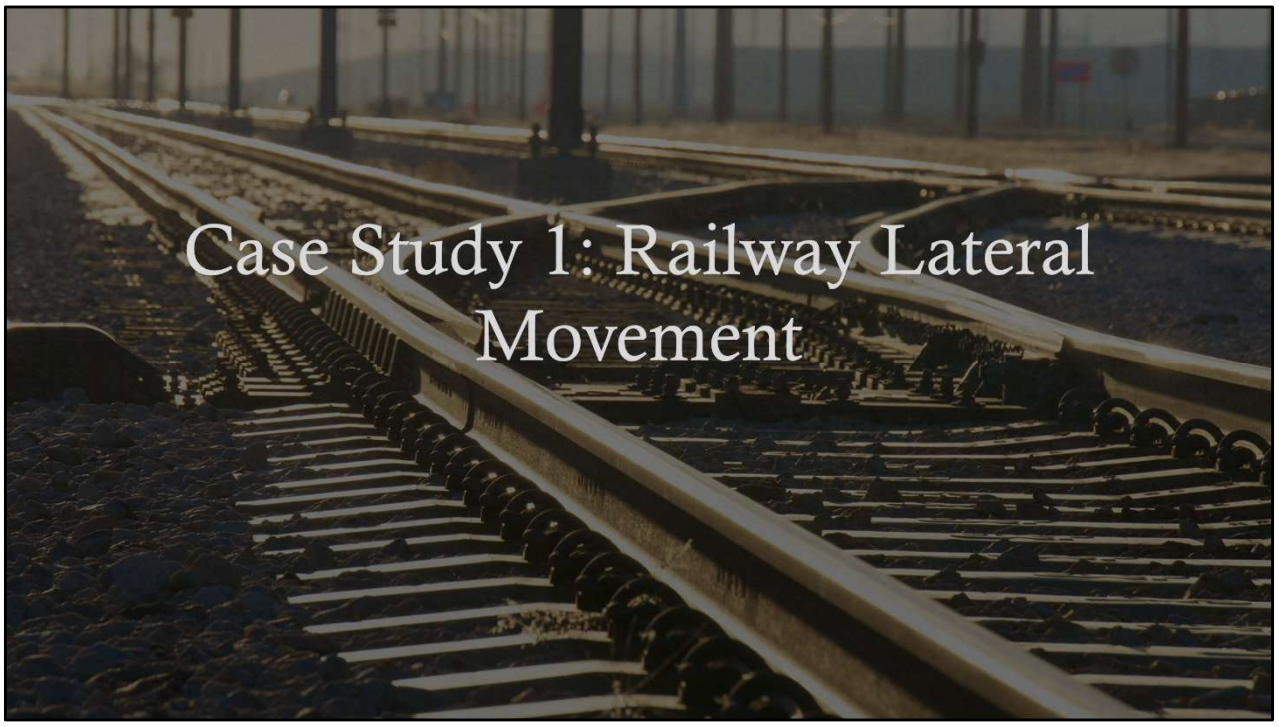
Legacy Systems

- Known vulnerable legacy systems in high-security zones
- Honeypots emplaced in lower security, or vulnerable zones
- Deceive attackers to target "easier" system allowing data gathering



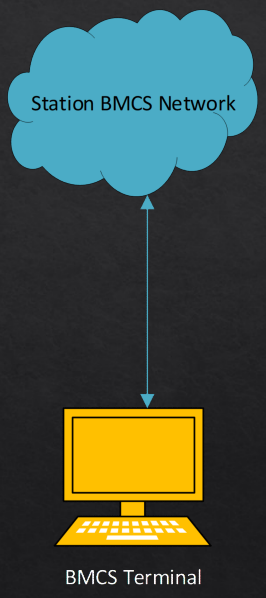
Agenda

Brief History | Purpose | Types | Use Cases | **Examples** | Global Use | How?


Case Study 1: Railway Lateral Movement

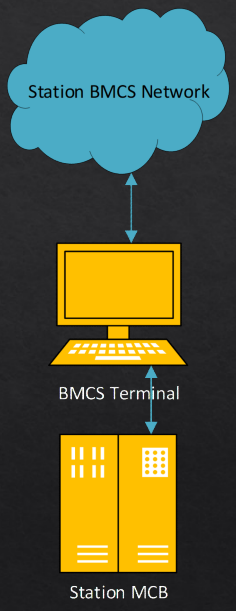
Setup

- New train station as part of a passenger line expansion
- Systems commissioned with minimal cybersecurity requirements or testing
- Station BMCS had local HMI for monitoring/command of:
  - Station Low Voltage (incl UPS)
  - Environmental
  - Vertical Transport
  - Hydraulics



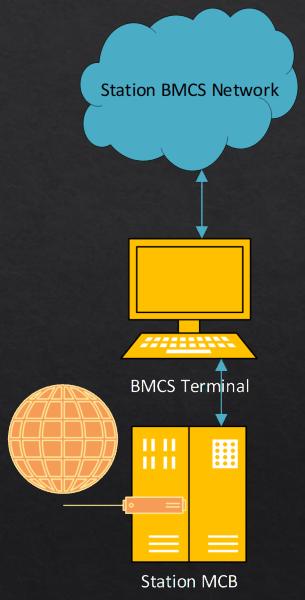
Vulnerability

- Assessment post commissioning identified potential vulnerability in Main Switch Boards at the station



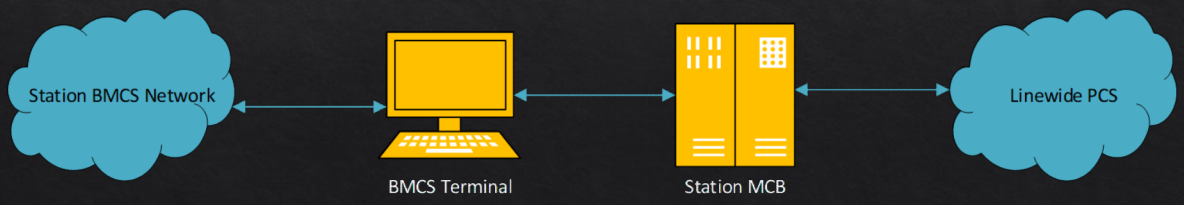
Vulnerability

- Assessment post commissioning identified potential vulnerability in Main Switch Boards at the station
- Switch Boards had a web service running that accepted file uploads (ie, webshell)



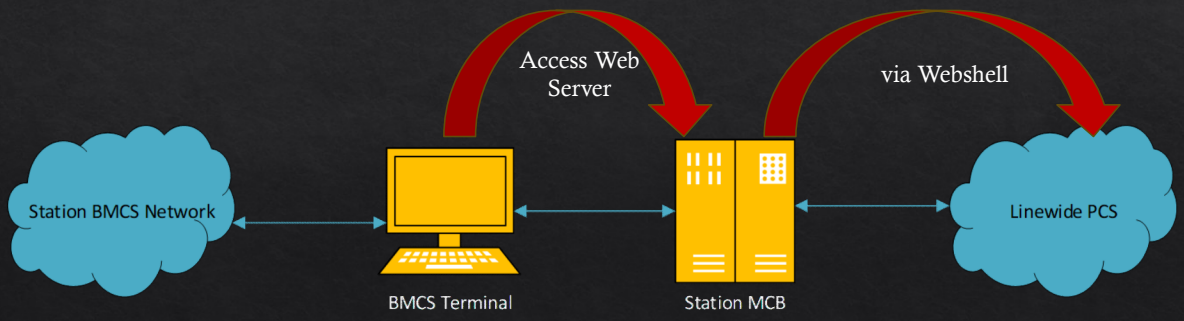
Lateral Movement Risk

- BMCS HMI could access MSB
- MSB had network access to Linewide PCS



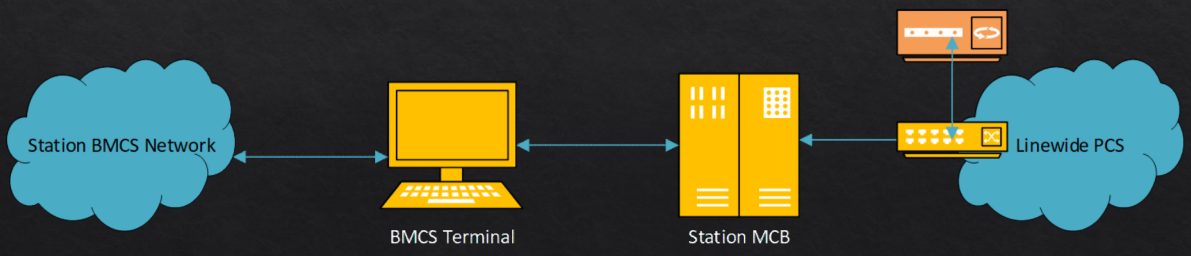
Lateral Movement Risk

- BMCS HMI could access MCB
- MCB had network access to Linewide PCS



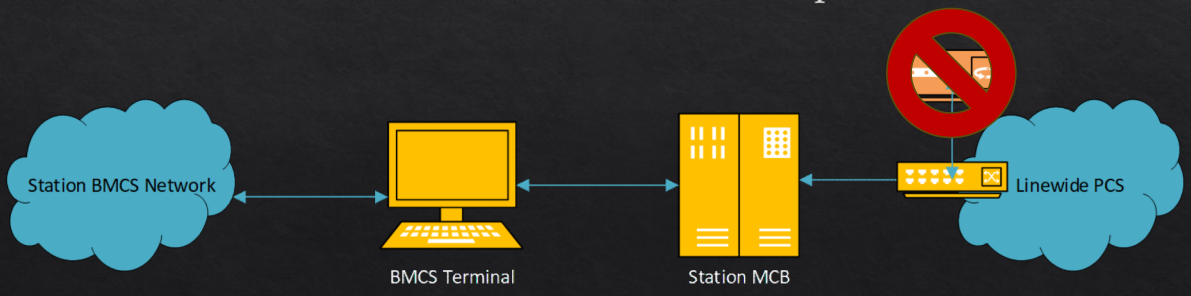
Monitoring Limitation

- BMCS HMI could access MCB
- MCB had network access to Linewide PCS
- Deployment of NIDS was considered for the PCS network



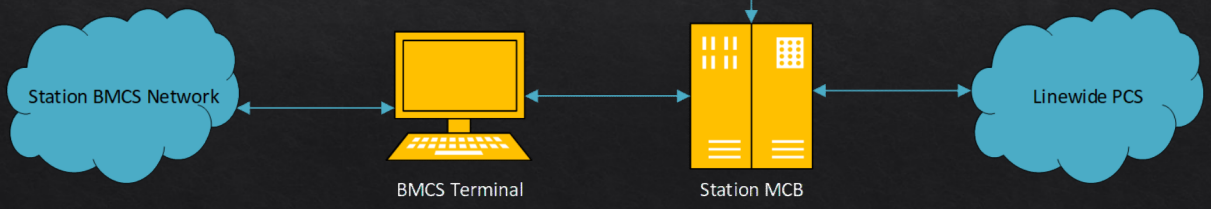
Monitoring Limitation

- BMCS HMI could access MCB
- MCB had network access to Linewide PCS
- PCS network could not accommodate SPAN ports



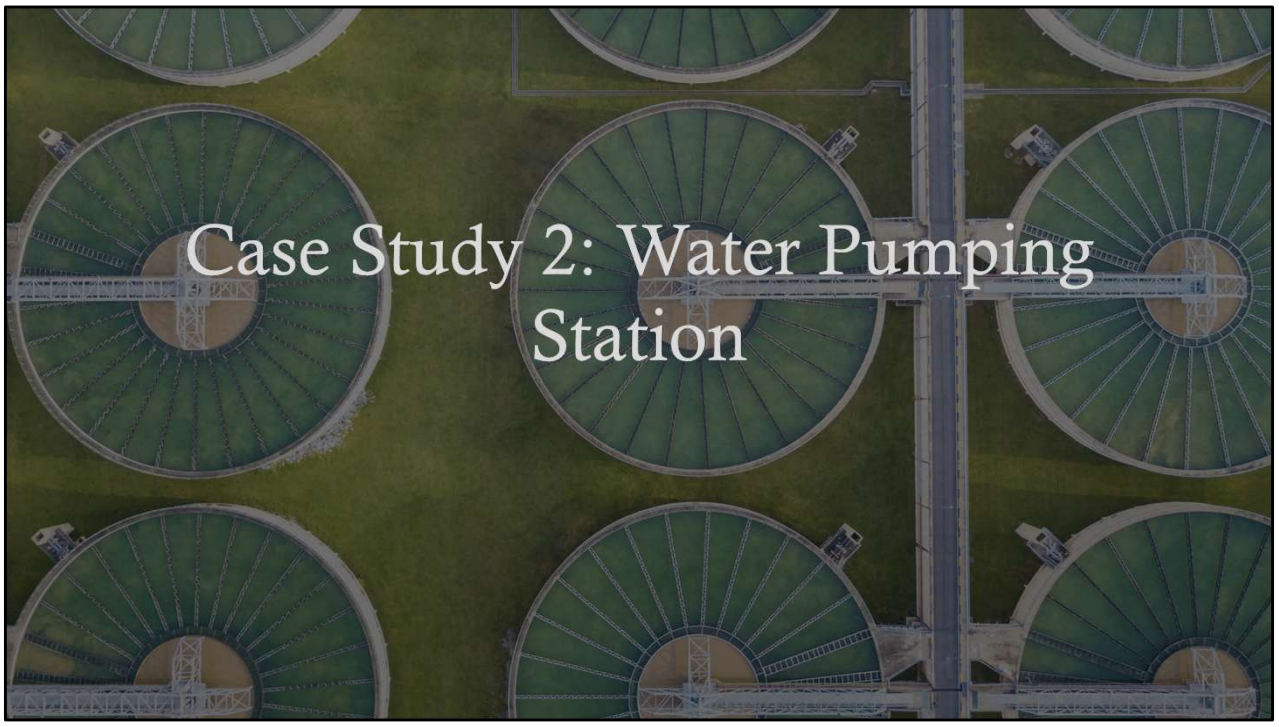
Honeypot Deployment

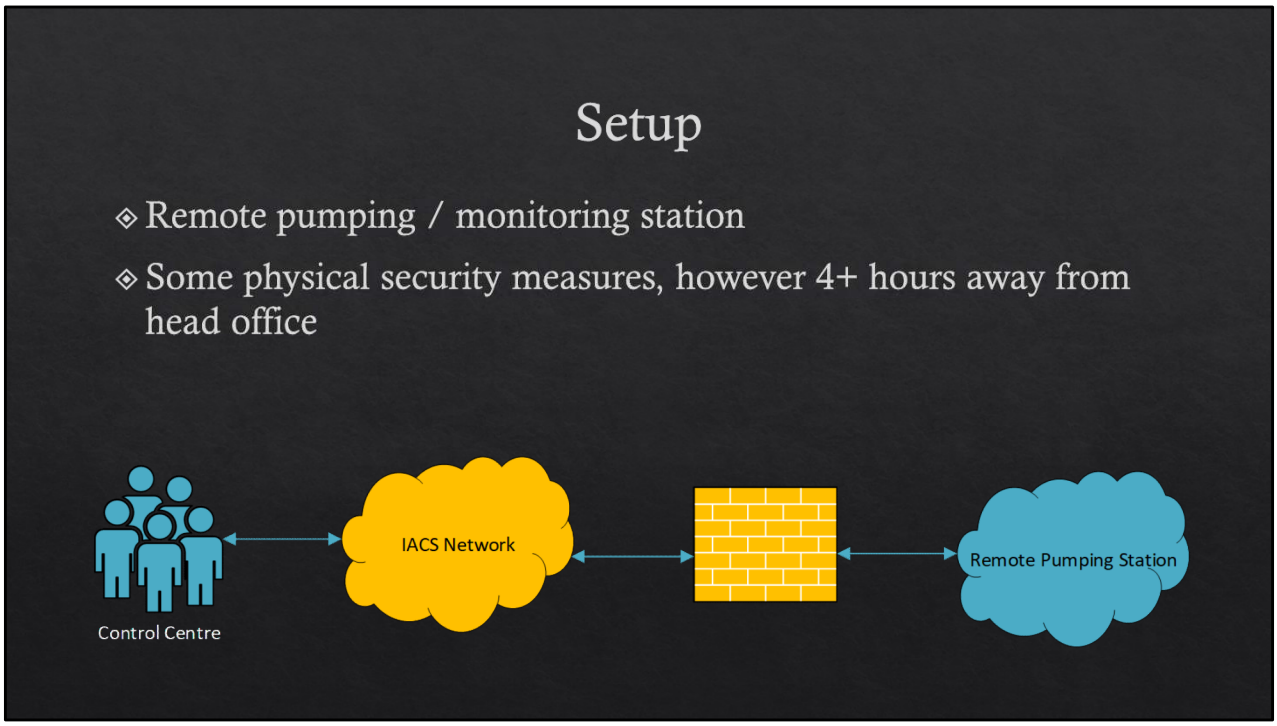
- Honeypot was deployed to PCS network and exposed to MSB
- Ideally Honeypot would detect reconnaissance / lateral movement from MSB



Outcome and Benefits

- Interim monitoring solution was able to be put in place
- Defect remediation works to be conducted on MSB (update to remove web service)
- Upgrade to PCS network switched planned to accommodate expansion of NIDS deployment

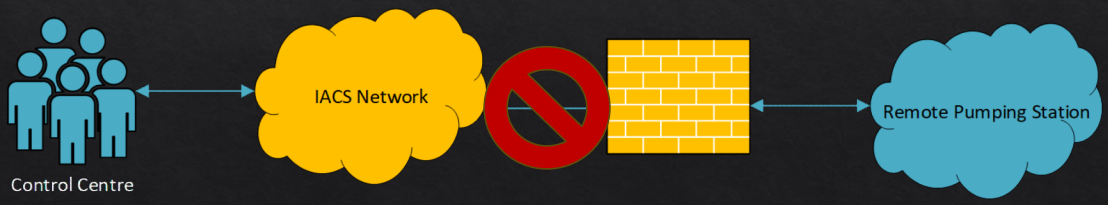

Case Study 2: Water Pumping Station



While working for MSSP SOC

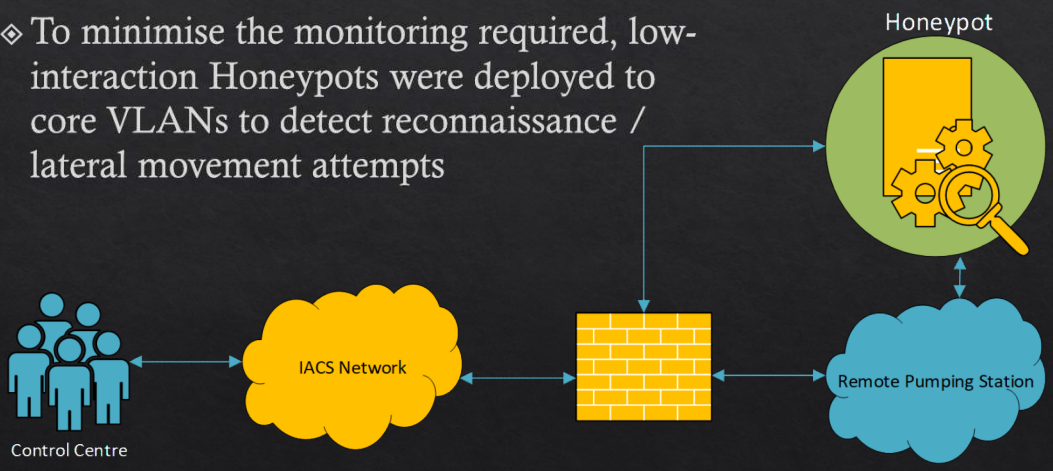
Setup

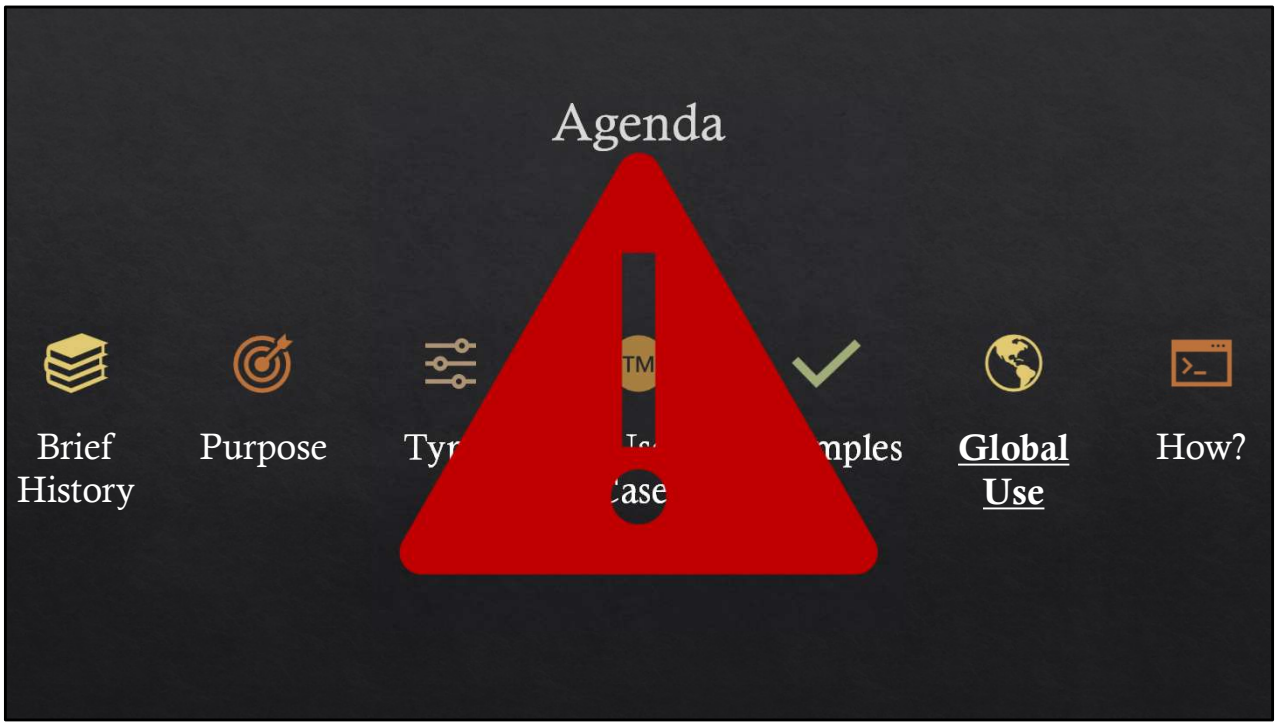
- Minimal bandwidth available for adequate monitoring of systems/servers on site
- Also – SIEM solution used was a data hog, American companies don't understand "low bandwidth"



Honeypot Deployment

- To minimise the monitoring required, low-interaction Honeypots were deployed to core VLANs to detect reconnaissance / lateral movement attempts




Agenda
Brief History
Purpose
Tyr
ase
mples
Global Use
How?

> ww-rps4-hp sshd[1234]: Failed password for invalid user root from 192.168.1.101 port 51123 ssh2

> ww-rps4-hp kernel: [UFW BLOCK] IN=eth0 OUT= MAC=02:42:ac:11:00:02:06:42:ac:11:00:03:08:00 SRC=192.168.1.101 DST=192.168.1.10 LEN=60 TOS=0x00 PREC=0x00 TTL=54 ID=54321 DF PROTO=TCP SPT=33333 DPT=22 WINDOW=14600 RES=0x00 SYN URGP=0

> ww-rps4-hp kernel: [UFW BLOCK] IN=eth0 OUT= MAC=02:42:ac:11:00:02:06:42:ac:11:00:03:08:00 SRC=192.168.1.101 DST=192.168.1.10 LEN=60 TOS=0x00 PREC=0x00 TTL=54 ID=54322 DF PROTO=TCP SPT=33334 DPT=23 WINDOW=14600 RES=0x00 SYN URGP=0

> ww-rps4-hp kernel: [UFW BLOCK] IN=eth0 OUT= MAC=02:42:ac:11:00:02:06:42:ac:11:00:03:08:00 SRC=192.168.1.101 DST=192.168.1.10 LEN=60 TOS=0x00 PREC=0x00 TTL=54 ID=54323 DF PROTO=TCP SPT=33335 DPT=80 WINDOW=14600 RES=0x00 SYN URGP=0

> ww-rps4-hp sshd[1234]: Failed password for invalid user admin from 192.168.1.101 port 51124 ssh2

> ww-rps4-hp telnetd[5678]: Connect failed: Unauthorized access attempt from 192.168.1.101 port 41111

Suspicious Activity Detected

- Activity was detected and raised as an incident by the SOC
- No changes identified which could cause incident
- No CCTV available (to SOC staff to corroborate), however pressure sensors triggered on cabinets on site
- Local Site Security Contractor contacted and directed to site

Outcome

- Local Contractor found a worker inside equipment room connected to local switch
- After coordination with client cybersecurity team, it was identified that worker had made an error when attempting to conduct a change (wrong asset information)

Lessons Learned

- Monitoring solution was validated (even though for a false positive)
- Cybersecurity Incident Response interface with physical security and change management teams reviewed
- Issues with asset inventory on site was identified (bonus!)

Agenda


Brief History


Purpose


Types

Use Cases

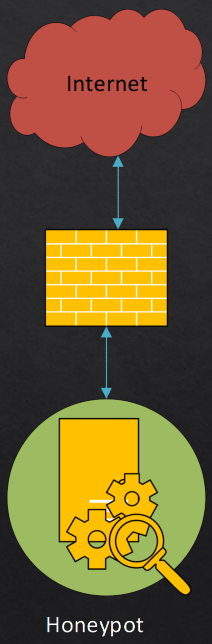

Examples


Global Use


How?

Deploying to the Edge

- Deploying to your environment edge you can gain unique information about who is potentially attacking you
- Honeypots on the edge will mostly see automated attacks ("noise of the internet")
- If you know what the "noise" is you can filter it out to find what is unique



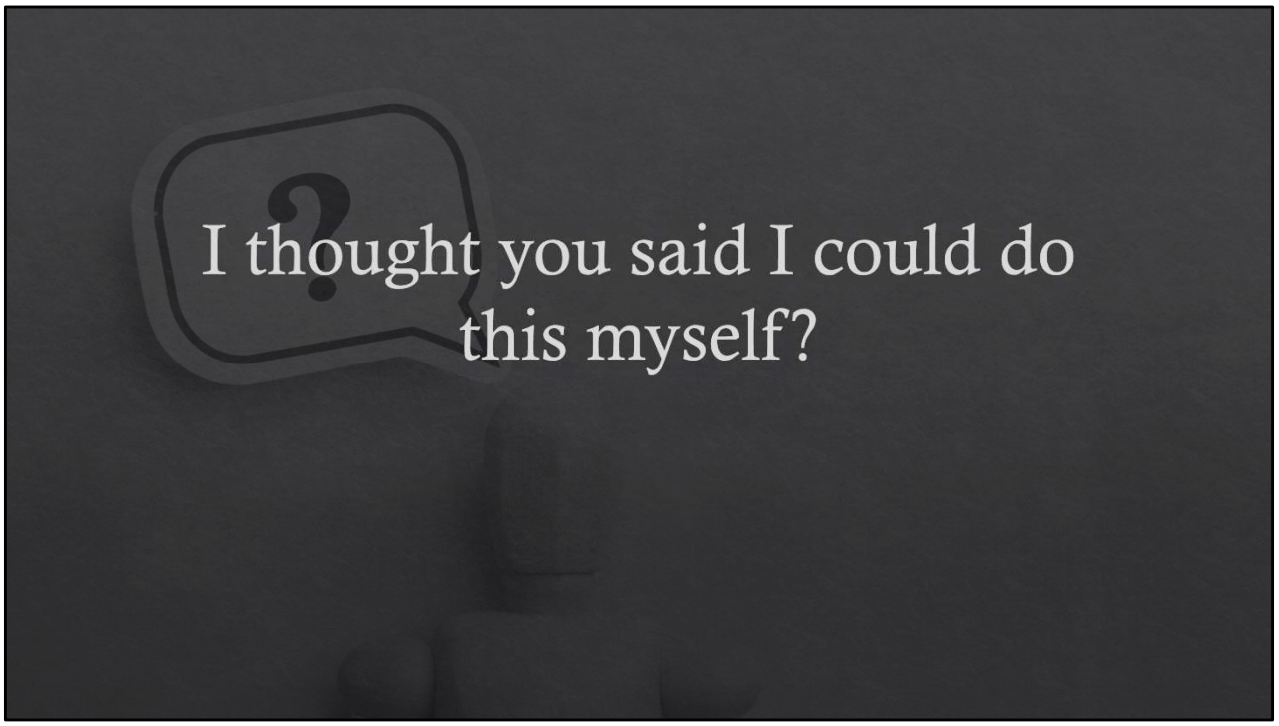
Generating the Noise

- Cloud deployment (Azure, AWS) can generate some noise
- Emplacing a honeypot at an office or commercial data centre can generate additional data
- Excluding known mass scanners from other sources

https://raw.githubusercontent.com/stamparm/maltrail/master/trails/static/mass_scanner.txt

Gaining a Global Context

- With more than one network (office, plant, site, etc) you can start to compare results seen between sites
- This allows us to see threats that are potentially directly targeting specific sites


I thought you said I could do this myself?

Agenda


Brief History


Purpose


Types

Use Cases


Examples


Global Use


How?

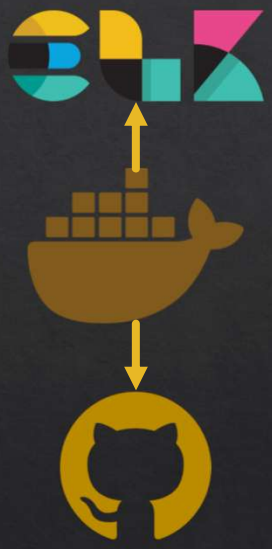
Where to Start?

Adbhoney	Elasticpot	Log4pot
Ciscoasa	Endlessh	Mailoney
Citrixhoneypot	Glutton	Medpot
Conpot	Hellpot	Redishoneypot
Cowrie	Heralding	Sentrypeer
Ddospot	Honeypots	Snare
Dicompot	Honeytrap	Tanner
Dionaea	Ipphoney	Wordpot


T-POT

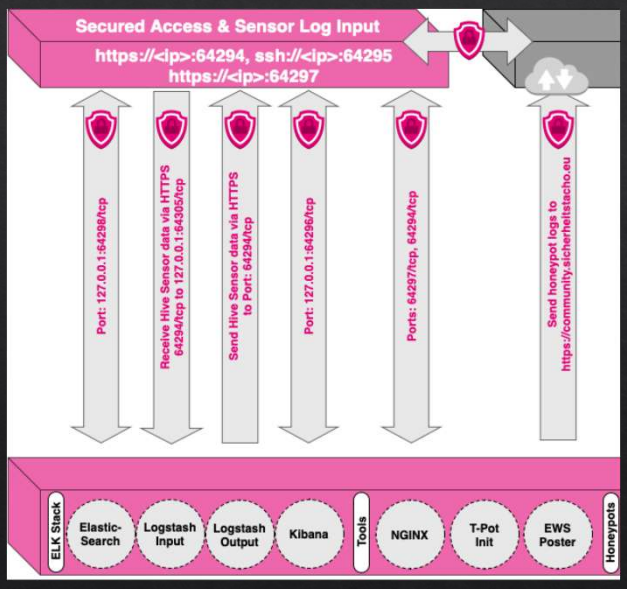
TPOT

- AiO Honeypot Platform
- Created by Deutsch Telecom
- Composed with Docker
  - Image for each honeypot
  - Logs are shipped to an ELK stack
  - Capable of managing distributed sensor deployment
- Sensor = 8GB RAM, 128GB SSD
  - Rpi4 w/ MicroSD card



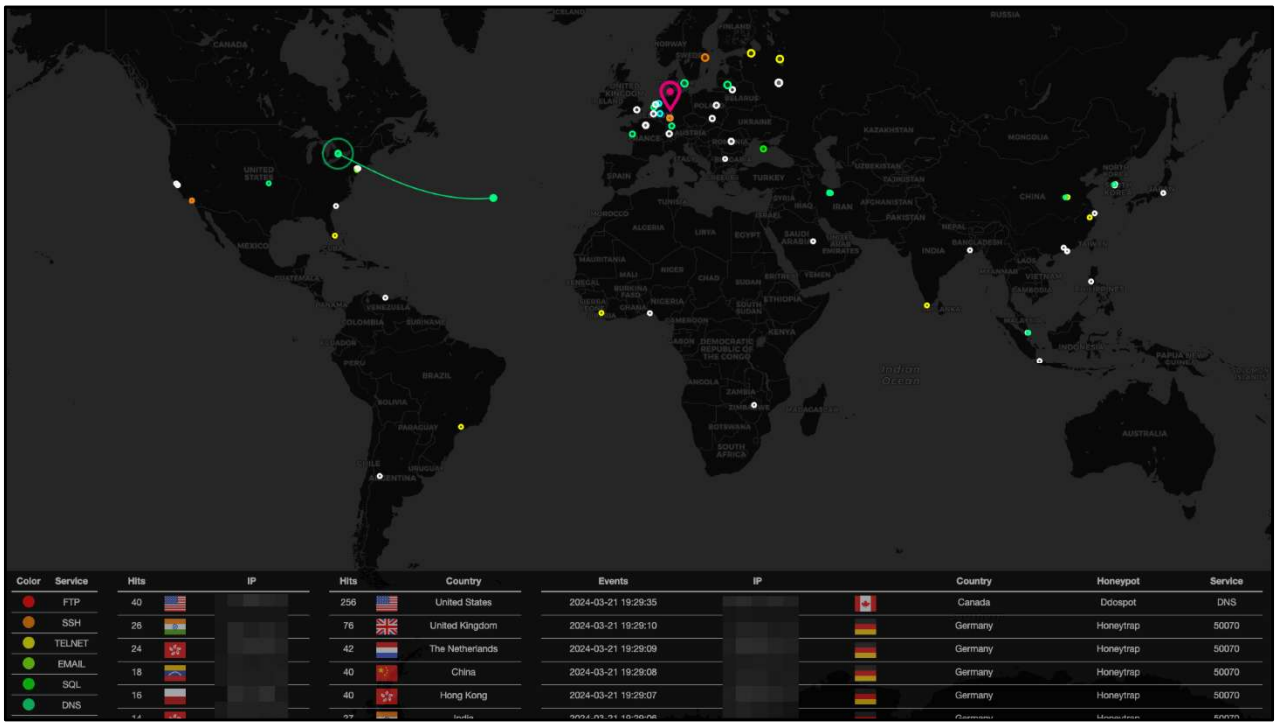
TPOT

- ELK services run on the honeypot device
- NGINX provides secure access on non-standard port
- Configuration can be done on appliance or remote



~~Where to Start?~~ ALL OF IT

Adbhoney	Elasticpot	Log4pot
Ciscoasa	Endlessh	Mailoney
Citrixhoneypot	Glutton	Medpot
Conpot	Hellpot	Redishoneypot
Cowrie	Heralding	Sentrypeer
Ddospot	Honeypots	Snare
Dicompot	Honeytrap	Tanner
Dionaea	Ipphoney	Wordpot



Color	Service
	FTP
	SSH
	TELNET
	EMAIL
	SQL
	DNS

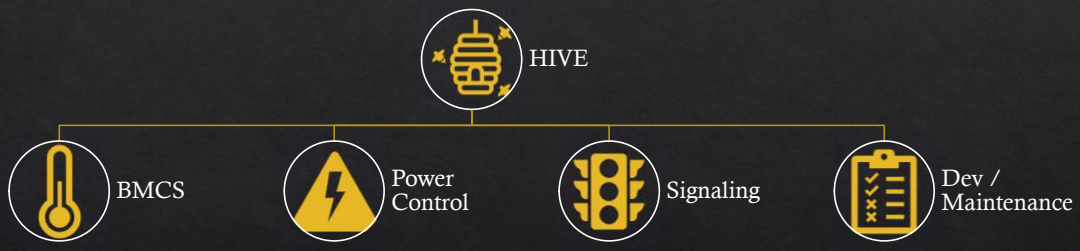
Hits	IP
40	
26	
24	
18	
16	

Hits	Country
256	United States
76	United Kingdom
42	The Netherlands
40	China
40	Hong Kong

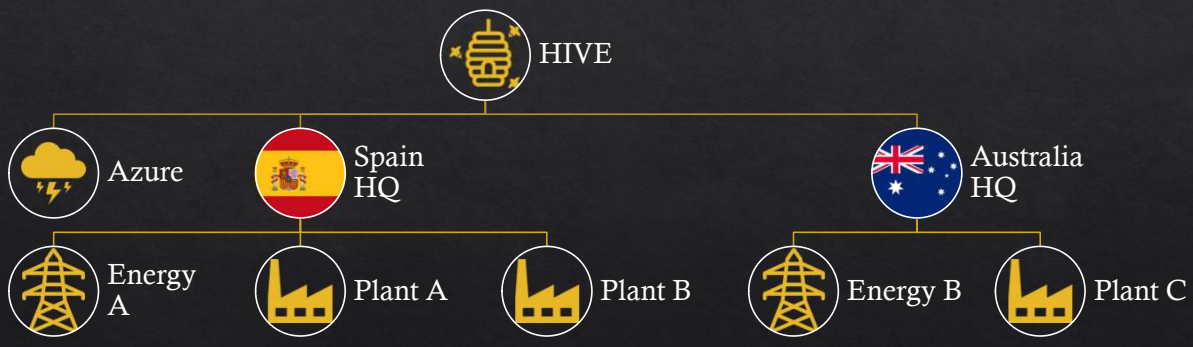
Events	IP	Country	Honeypot	Service
2024-03-21 19:29:35		Canada	Ddospot	DNS
2024-03-21 19:29:10		Germany	Honeytrap	50070
2024-03-21 19:29:09		Germany	Honeytrap	50070
2024-03-21 19:29:08		Germany	Honeytrap	50070
2024-03-21 19:29:07		Germany	Honeytrap	50070

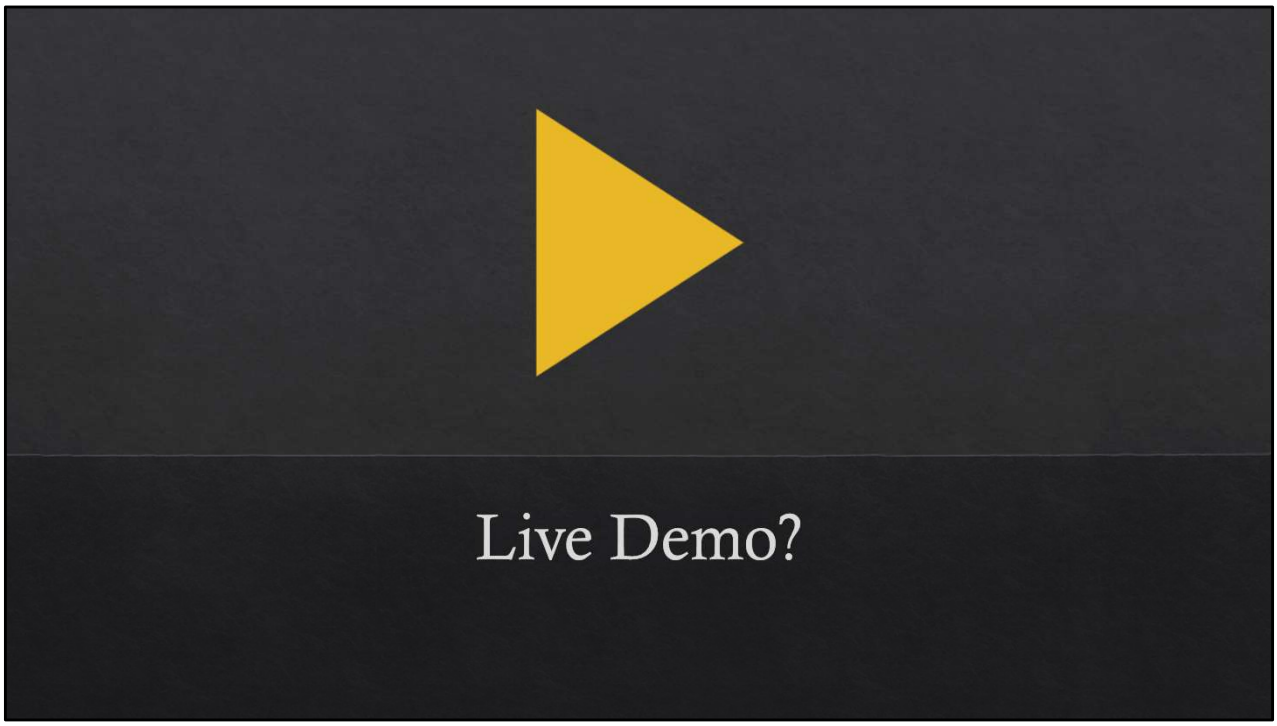

Honeypot Attacks
20,896
Honeytrap
Attacks
12,941
Cowrie
Attacks
5,209
Ddospot
Attacks
1,233
Malloney
Attacks
601
Redishoneypot
Attacks
267
Adbhoney
Attacks
241
Dionaea
Attacks
186
ConPot
Attacks
112
Ciscoasa
Attacks
31
Heralding
Attacks
28
Honeypot Attacks Bar
Honeypot Attacks Histogram
Attacks
Unique Source IPs
Attack Map - Dynamic
Elastic Maps Service
OpenMapTiles
OpenStreetMap contributors
Attacks by Destination Port Histogram
8000
7000
22
123
25
Attacks by Honeypot Histogram
Honeytrap
Cowrie
Ddospot
Malloney
Redishoneypot
Attacks by Country Histogram
United States
China
United Kingdom
Hong Kong
The Netherlands
Attacker Src IP Reputation
known attacker
mass scanner
bot, crawler
tor exit node
Attacks by Honeypot
Honeytrap
Cowrie
Ddospot
Malloney
Redishoneypot
Adbhoney
Dionaea
ConPot
Ciscoasa
Heralding
P0f OS Distribution
Linux 2.2.x-3.x
Windows 7 or 8
Mac OS X
Linux 3.11 and newer
Windows NT kernel
Linux 3.1-3.10
Linux 2.4.x
Windows XP
Attacks by Country
United States
China
United Kingdom
Hong Kong
The Netherlands
Russia
United Arab Emirates
Germany
Bulgaria
Botswana
Attacks by Country and Port
Suricata Alert Category Histogram
Generic Protocol Comm...

Distributed Deployment



Distributed Deployment




Live Demo?


Key Takeaways

Key Takeaways for Honeypot Deployments

Honeypots provide critical visibility in environments where traditional security controls are impractical.

By leveraging different types of honeypots, organizations can monitor both internal and external threats effectively.

Multinational deployments enable organizations to understand global vs. regional threat patterns and detect targeted attacks.

The Role of Honeypots in Active Defence

Detect unusual activity before it reaches critical systems.

Gather valuable data on attacker behavior, including reconnaissance and lateral movement attempts.

Honeypots can be a cost-effective solution where full security controls aren't feasible.

Key Considerations for Deployment

Choose the right honeypot type based on environment needs and security goals.

Proper placement is crucial to ensure honeypots are in positions where they can capture relevant data.

Regularly review honeypot data and update configurations as threats evolve.

THANK YOU

https://github.com/telekom-security/tpotce

https://github.com/Oscar-Geare/presentations-and-papers