**Intro to Threat Detection - Honeypots**

**Honey Pots**

Used to detect threats, placed in sensitive areas where a threat shouldn’t be

* Appears to contain valuable information but is actually an isolated honey pot used to alert you

The Ideal Honeypot

* Fast and easy to deploy
* Discoverable to your threats
* Deployed in sufficient numbers or density
* Deployed in the right locations
* Produce high quality signals of the threat presence (low/no false alarms)
* Virtually no management
* Reliable

**Canary Tokens**

Email alerts for file access

Places a web bug in a file that is activated when the location is accessed

Many different types of tokens

* Word documents
* Web bugs
* PDF
* EXE/DLL
* SQL server alert
* QR code
* Remote image
* Directory browsing
* SVN token
* HTTP/DNS tokens

Add key words like ‘passwords’, ‘bitcoin’, ‘secret phrase’ etc. to bait the hacker

Malware performs a lot of sc m anning so you would want your canaries to be caught by that

**OpenCanary**

Linux tool to create custom canaries

* Can create cmds e.g., use a throwaway email for alerts but forward to a used email so you actually see the alerts

**Artillery**

A honey pot, file monitoring and overall security tool used to protect nix systems