High fidelity detection with honeypots

Don’t search for your adversary, let them come to you

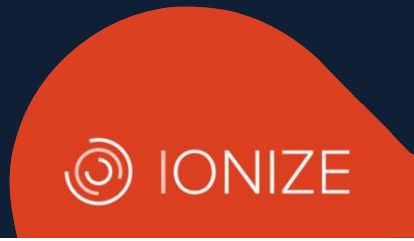
Andrew Muller, Ionize

TLNOG2 21st November 2025

IONIZE

Introduction

- We are constantly trying to detect malicious activity. Living off the land techniques make this very difficult.
- So why look for adversaries when they can come to you?
- Honeypots are not new. Now called "deception technology" because honeypots didn't sound cool enough.
- This talk will explore cheap and easy ways to get started.



Cyber adversaries

Adversary type	Motivation	Target
Cybercriminals (Organised Crime)	Financial Gain	Anyone
Nation-State Actors (APT Groups)	Espionage, Political Advantage, Sabotage, Military/Strategic Advantage	Government, government contractors, critical infrastructure, high-tech research
Hacktivists	Protest	Government, controversial organisations
Malicious Insider	Revenge, Financial Gain, or Intellectual Property	Current employer
Competitors	Intellectual Property	Competitors

Honeypots

Not new

- First mentioned in 1980's
- The Honeynet Project (1999)
- Evolution in broader deception technologies
- Lots of options
  - Server, network honeypots
  - Low interaction, high interaction
  - Honeytokens

Honeypot Strategies

What are you worried about?

- Focus on your most valuable assets
- Focus on who wants them and most likely to get them
- Build honeypot to attract them

Cybercriminals

What are you worried about?

- Will briefly look around network then cryptolocker it
- Honeypots unlikely to help

Nation-State Actors

What are you worried about?

- Will look have detailed look at network
- Common honeypots will be identified
- Honeytokens best and easy option
- Create a SECRET or CONFIDENTIAL folder and alert when its accessed

Hacktivists

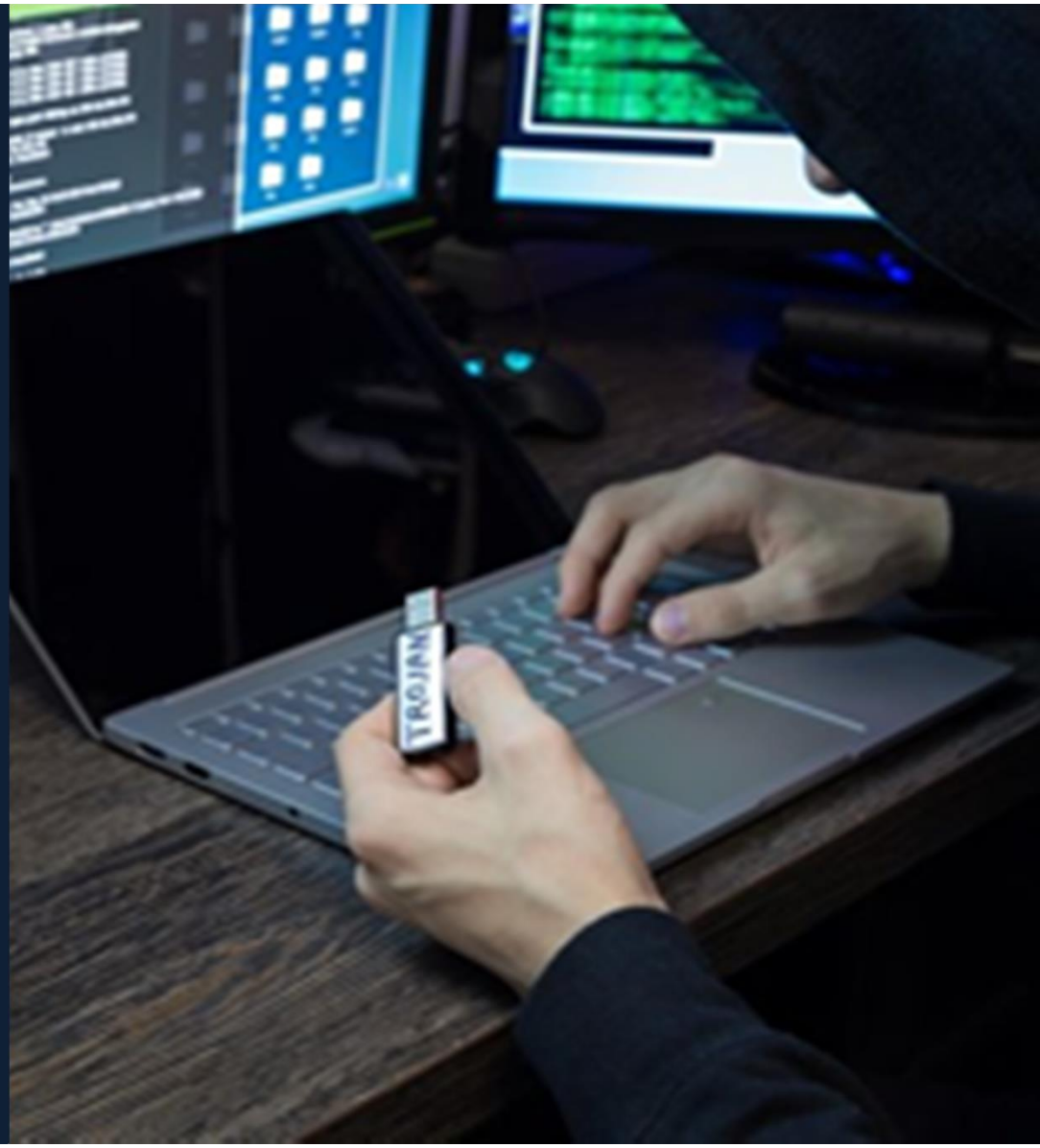
What are you worried about?

- Will have detailed look at network
- Common honeypots won't be identified
- Honeytokens best and easy option
- Create a SECRET or CONFIDENTIAL folder and alert when its accessed

Malicious Insider

What are you worried about?

- Will have detailed look at network
- Common honeypots won't be identified
- Honeytokens best and easy option
- Create a SECRET or CONFIDENTIAL folder and alert when its accessed



Competitors

What are you worried about?

- Will have detailed look at network
- Common honeypots won't be identified
- Honeytokens best and easy option
- Create a SECRET or CONFIDENTIAL folder and alert when its accessed

How?

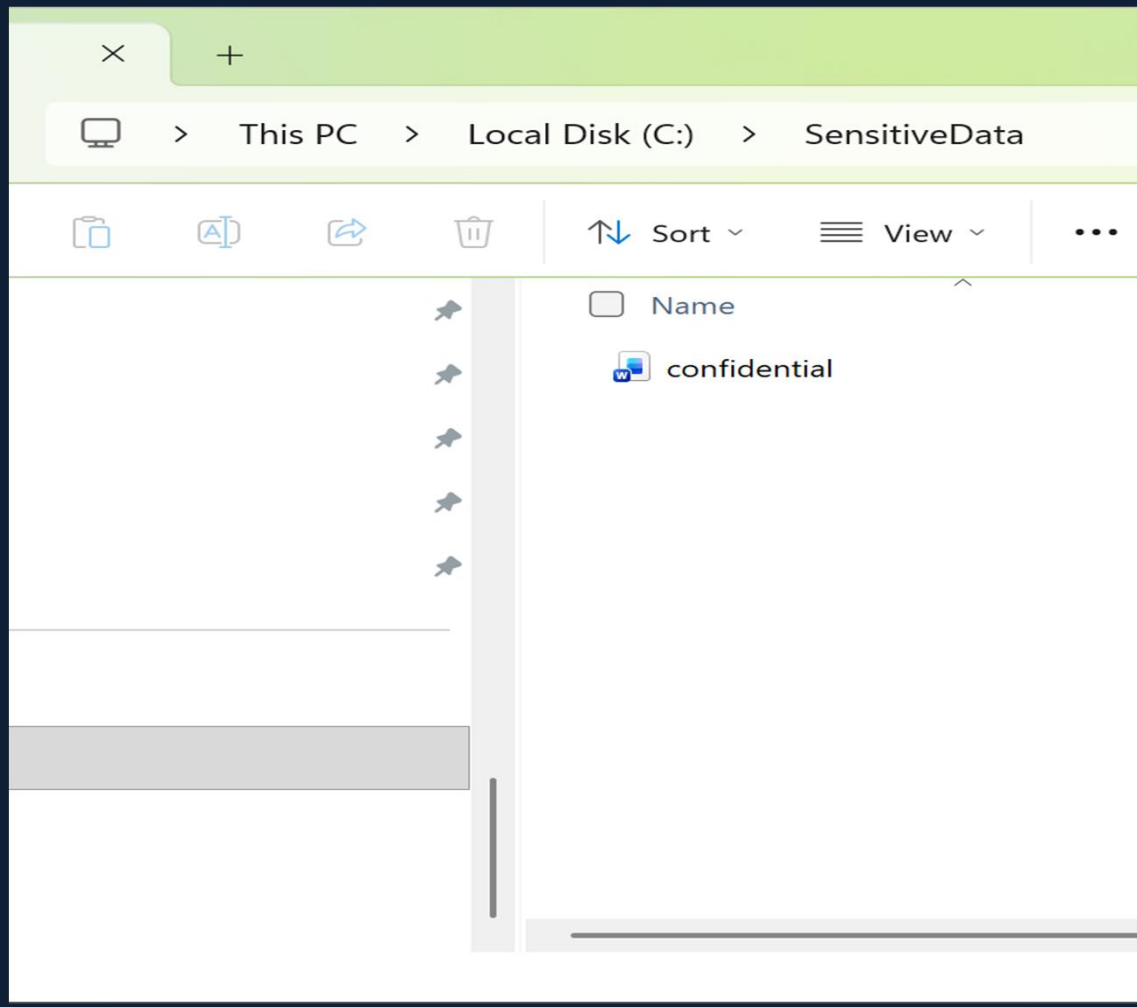
Keep it simple

- Set a trap with something desirable
- Use a honeytoken
- Create a folder or file labeled SECRET or CONFIDENTIAL and fire an alert when its accessed

Example

Create a honeytoken

- Create a SECRET or CONFIDENTIAL folder

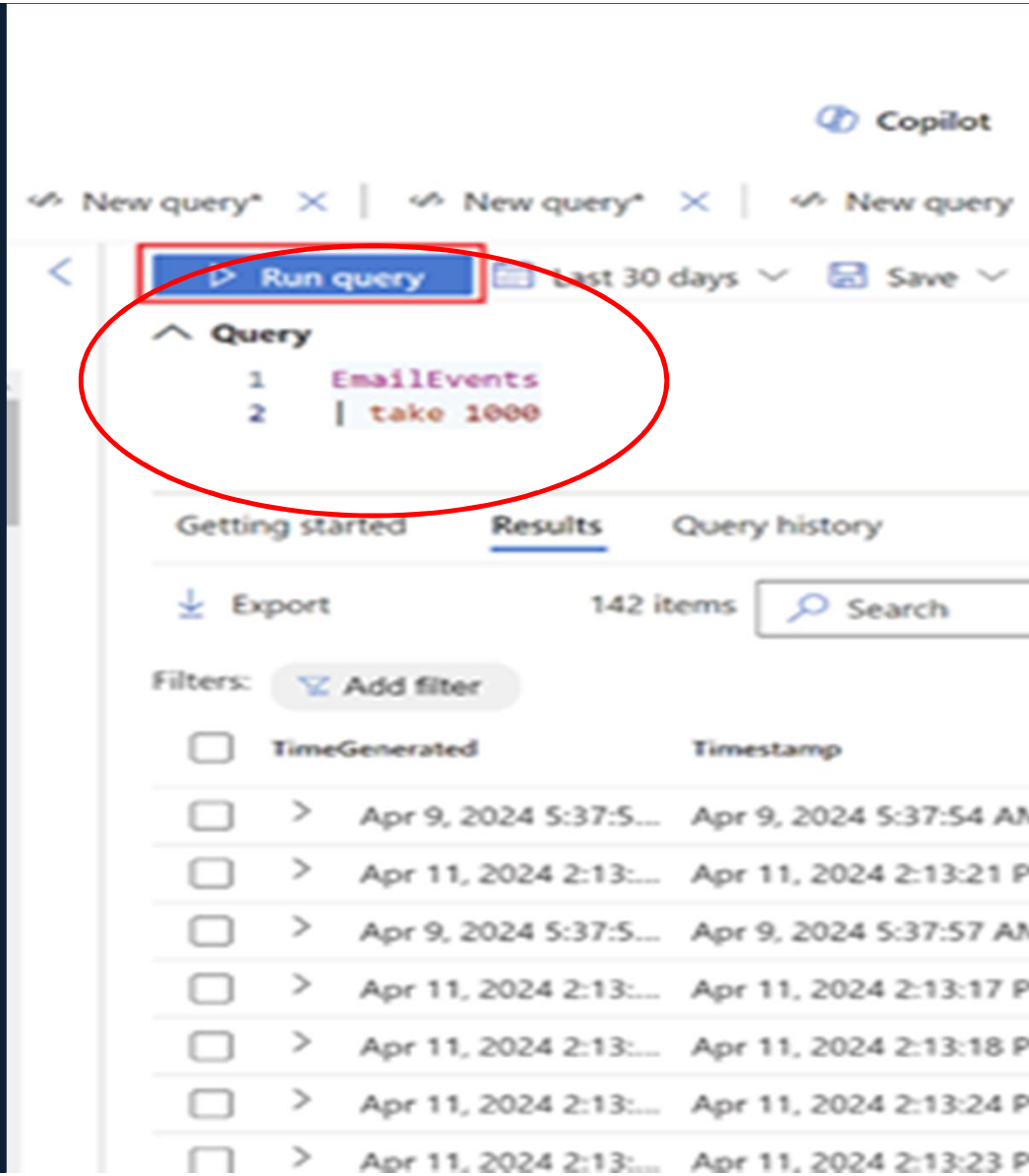


Example

Create an alert

- Create an alert when its accessed

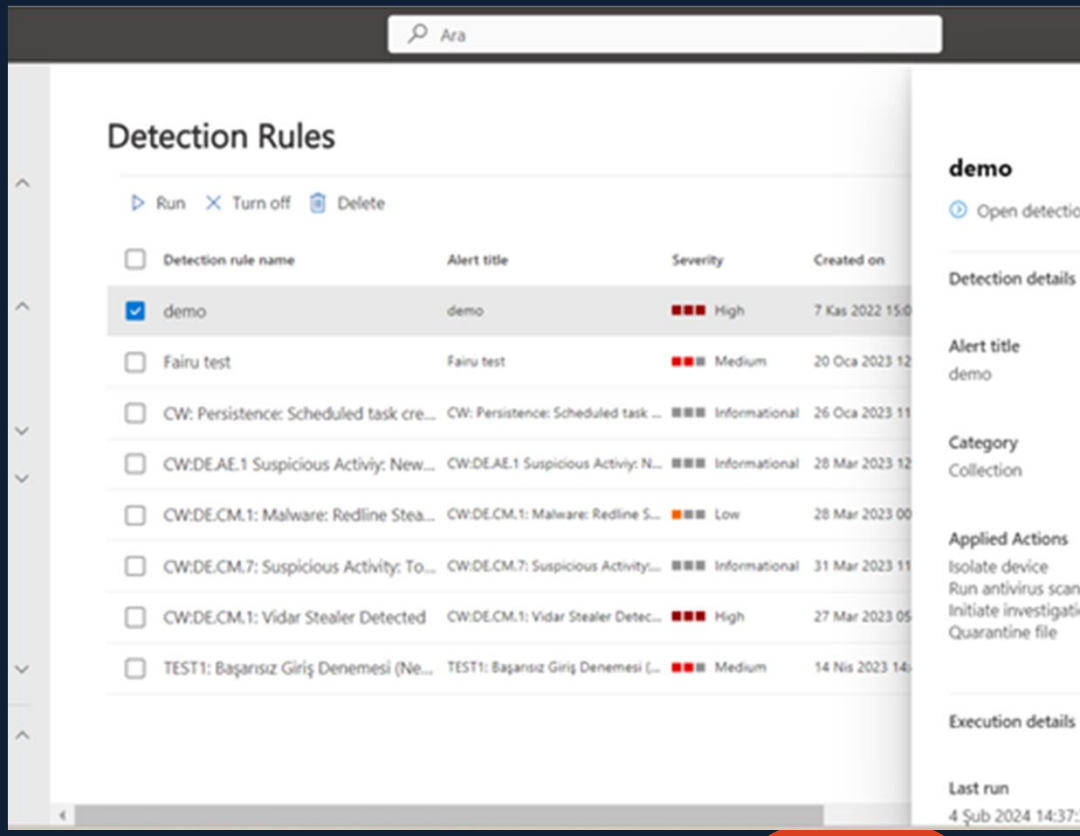
```
let targetFile = @"C:\SensitiveData\confidential.docx";
DeviceFileEvents
| where Timestamp > ago(7d)  // Search last 7 days
| where ActionType == "FileAccessed"  // Only file access events
| where FileName == "confidential.docx"
   or FolderPath =~ targetFile
| project Timestamp, DeviceName, InitiatingProcessAccountName, FolderPath, FileName, InitiatingProcessFileName, ReportId
| order by Timestamp desc
```



Example

Setup alert

- Setup up a KQL alert to trigger when its accessed.



IONIZE

Thank you.