


# Sandbox

Cyber Security Foundation Course

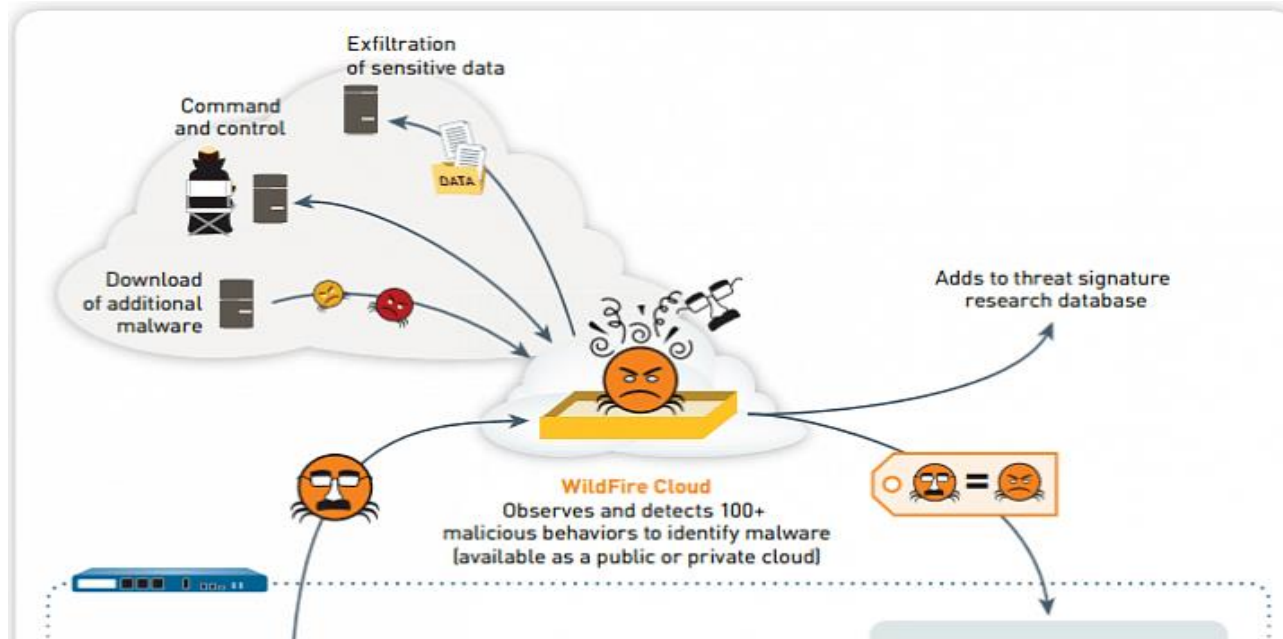
A large, irregular watercolor splash in shades of blue, purple, and green, centered on the left side of the slide. The word 'AGENDA' is written in white, bold, sans-serif capital letters across the center of this splash.

# AGENDA

- Definition
  - Sandbox Implementations
  - Sandbox Types
  - Sandbox Advantages
  - Sandbox disadvantages
- 
- A decorative footer consisting of numerous small, scattered blue and cyan ink splatters and dots along the bottom edge of the slide.

# Sandbox Definition

An Isolated environment maybe a computer, laptop, virtual machine, or Mobile device. To test the untrusted applications and executables before running it on the real environment. Also, several cybersecurity teams use it to know about the malware's behavior.



# Sandbox Implementations

- **Full system Emulations:** Use a real Machine not virtual machine to examine the suspicious programs.
- **Virtual System:** Use a virtual machine (VM) to examine the suspicious programs.



# SandboxTypes

- **Cloud Sandbox:**
  - AnyRun (<https://any.run/>)
  - Hybrid Analysis (<https://www.hybrid-analysis.com/> )
- **on premise malware sandbox**
  - Cuckoo sandbox (<https://cuckoosandbox.org/> )
- **Attached to another Security Appliacne such as (Email Gateway, Proxy, NGFW).**

# Sandbox Advantages:

- **Test and analyze untrusted applications before running it in production**
- **Allow security folks to know more about the malware behavior**

# Sandbox disadvantages:

- **Weak configuration could lead to Infect the real environment**
- **There are several Sandbox evasion techniques used by malware**



# Thanks!

Any questions?

