**Sandboxing in Cybersecurity: 3 Technologies:**

In cybersecurity “sandboxing” is a way to safely test or run software without risking the rest of the system. I think this is one of the smartest ways to deal with unknown threats, especially when working with malware or untrusted applications.

**3 common sandboxing technologies and how they work:**

1. Virtual Machines

A virtual machine is like a computer inside a computer. It runs its own operating system and behaves like a separate device. Security teams often use VMs to open suspicious files or run unknown programs. If something goes wrong, the damage stays inside the VM and doesn’t affect the real system.

*Strengths:*

* Full isolation from the host system
* Can simulate different operating systems
* Great for malware analysis

*Applications*:

* Used by SOC analysts to test malware behavior
* Helps developers test software in different environments

1. Application Sandboxing (AppArmor, Windows Sandbox)

This method restricts what an application can do. For example, it might block access to certain files, limit network usage, or prevent the app from installing anything. Windows Sandbox is a good example - it lets you run a program in a temporary environment that gets deleted when you close it.

*Strengths:*

* Lightweight and fast
* Built into many operating systems
* Good for everyday protection

*Applications:*

* Running untrusted apps safely
* Preventing apps from accessing sensitive data

1. Cloud-Based Sandboxing

Some companies use cloud services to analyze files. The file gets uploaded to a secure server, where it’s opened and tested in a controlled environment. This is often used by antivirus software and email security platforms.

*Strengths:*

* Doesn’t use local resources
* Fast and scalable
* Can analyze many files at once

*Applications:*

* Email filtering (checking attachments)
* Antivirus scanning
* Enterprise threat detection

Sandboxing is a key part of modern cybersecurity. Whether it’s through virtual machines, restricted apps, or cloud services, the goal is the same: keep threats isolated and protect the system. I think every SOC team should understand these tools.