|  |
| --- |
| [Nom de la société] |
| Vulnerability Management |
| [Sous-titre du document] |

|  |
| --- |
| Abdallah Chbaro  10/04/2023 |

# Life Cycle

The vulnerability management lifecycle is a process intended for organizations to effectively identify, remediate, and confirm the elimination of network vulnerabilities in a computer system.

This cyclical structure is not only designed for security professionals to address a vulnerability from start to finish but can be applied to any vulnerability instance.

For reliable, Continuous vulnerability management, following a lifecycle process is key to any organization’s security program.

# Frameworks For Vulnerability Management

Selecting a framework for your vulnerability management plan can provide a reference for designing and implementing security mechanisms to help ensure vulnerabilities to your organization are eliminated properly.

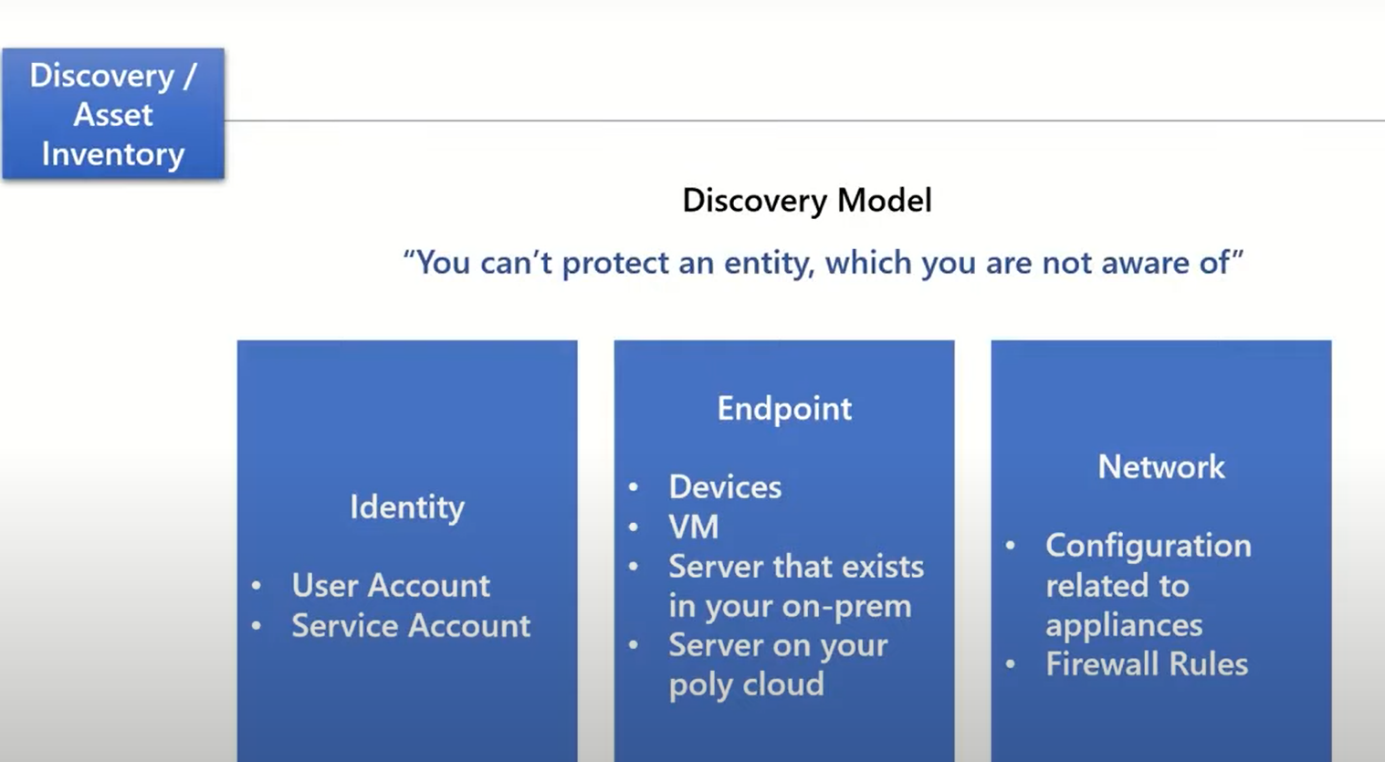
This assurance allows managers and leadership to intelligently manage their organization’s security posture using risk-based vulnerability management.

Abiding by a vulnerability management framework also instills confidence in the organization’s industry and establishes a strong reputation of proactive compliance, which can lead to increased business.



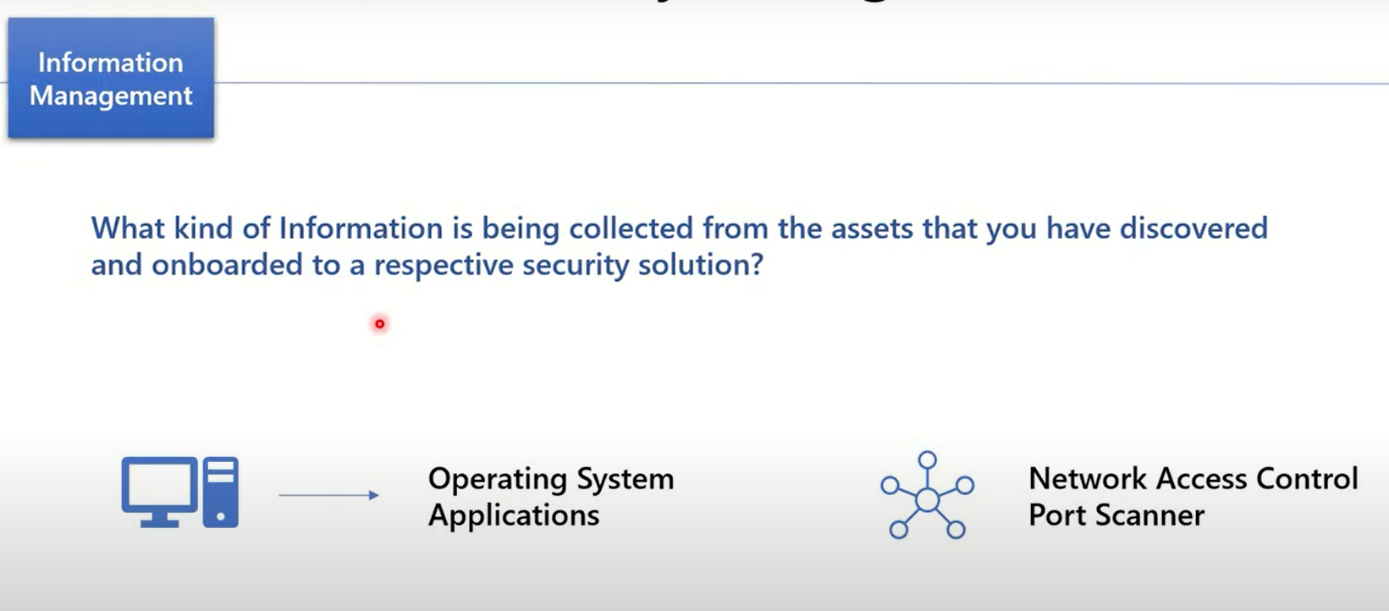
# Step 1 – Discovery / Asset Inventory

The most straightforward way to find a vulnerability is to scan your network and to conduct a vulnerability assessment. However, the first step is to know your assets.



# Step 2 – Information Management

The second step is to know the information you are collecting from your assets. For example, are you only scanning operating systems vulnerabilities? Are you scanning websites, IPs and APIs? Are you scanning network vulnerabilities also, such as protocols?

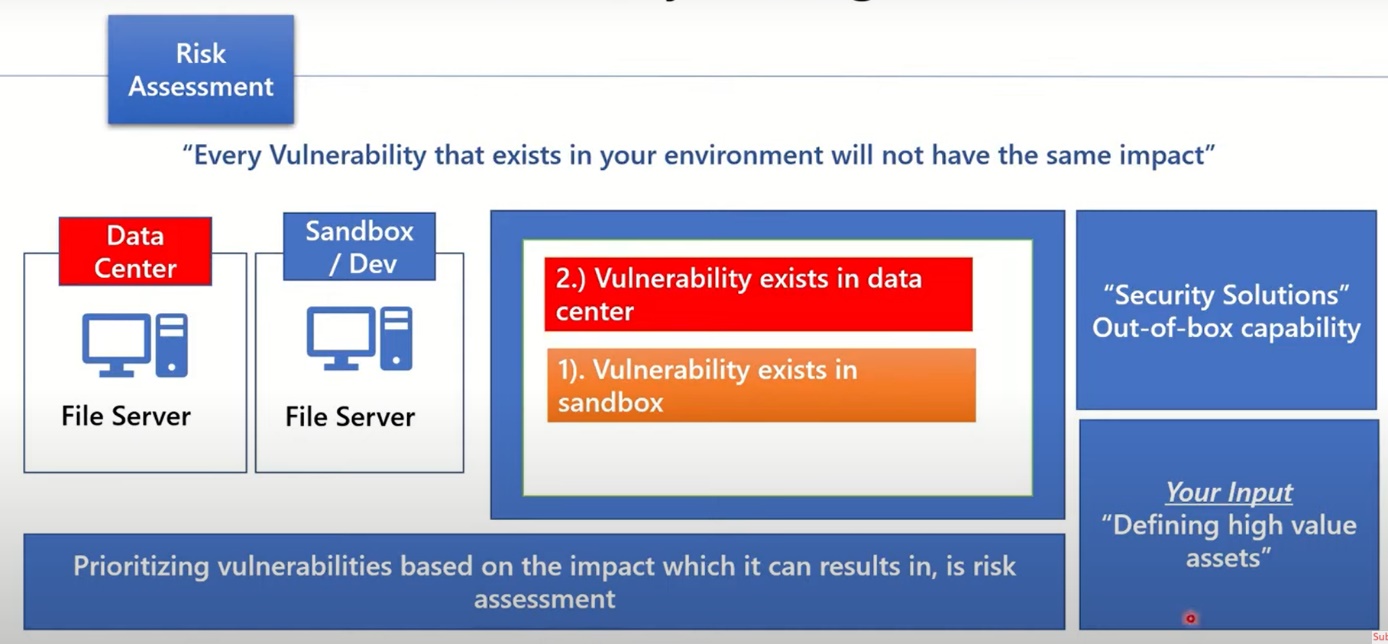


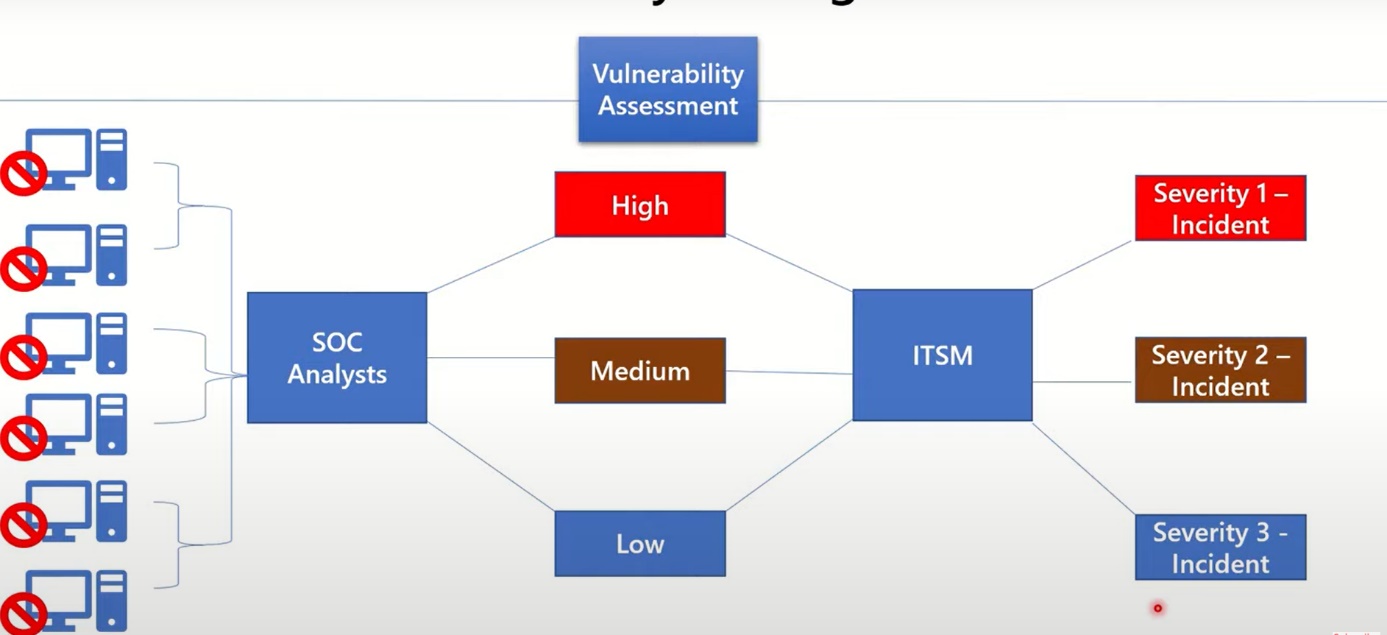
# Step 3 – Risk Assessment

The third step is to assess risk, for example you can base yourself on the following matrix:



 Not only this, you need to analyze if the risk has an impact on your system. For example, a high risk that has a low impact might be addressed lately and a low risk with high impact should be addressed immediately.

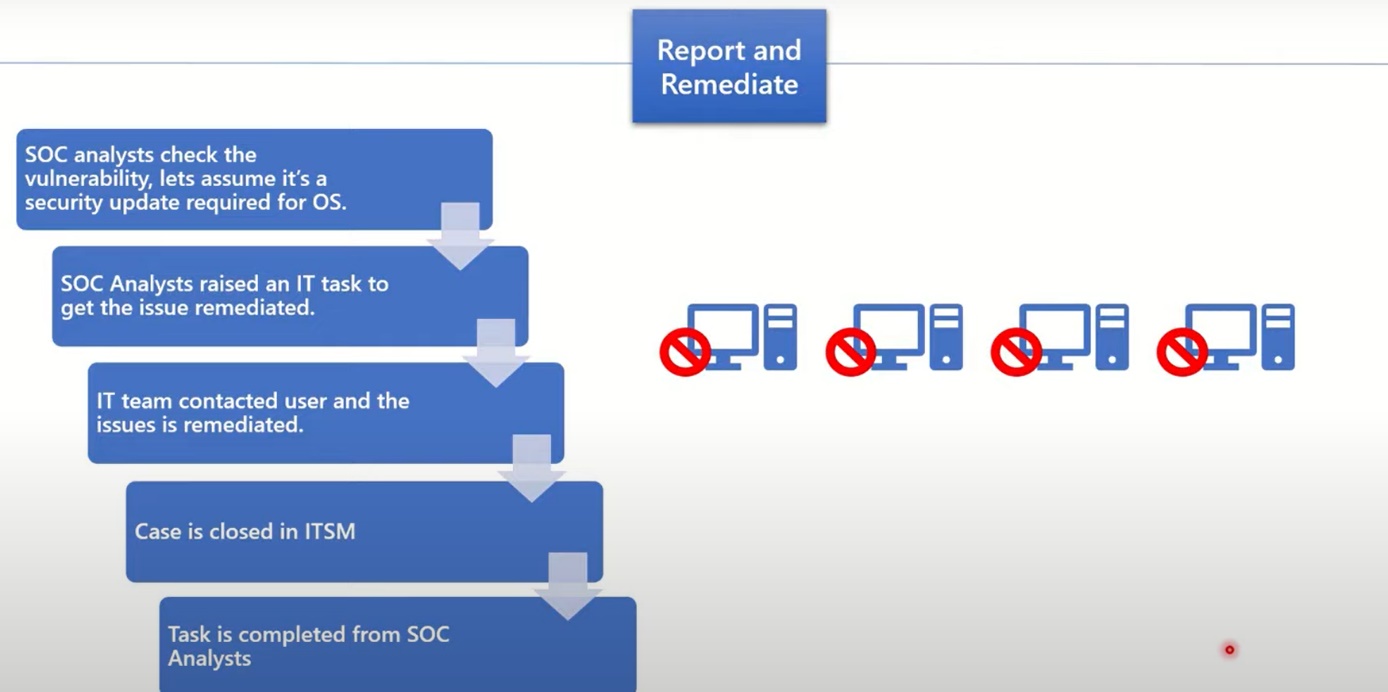


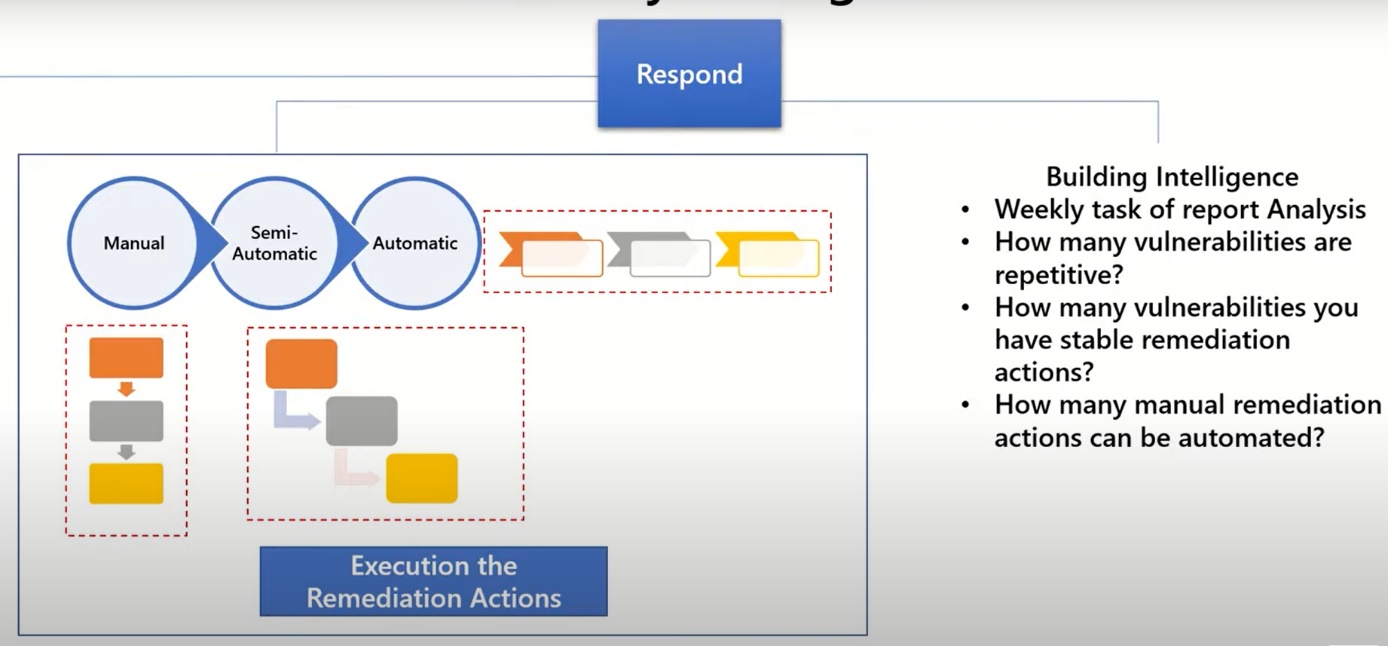


# Step 4 – Risk Mitigation

As for risk mitigation, you need to decide based on the analysis made earlier. The following strategies can be used:

* Risk avoidance
* Risk acceptance and sharing
* Risk mitigation
* Risk transfer





# Top Vulnerability Scanners

1. Acunetix
2. Burp Suite (Web Vulnerability Scanner)
3. Nessus (Web scanner from Tenable)
4. Tenable (Web + Network)
5. Nexpose
6. Qualys Guard
7. ZAP (Open Source)
8. OpenVas (Open Source)