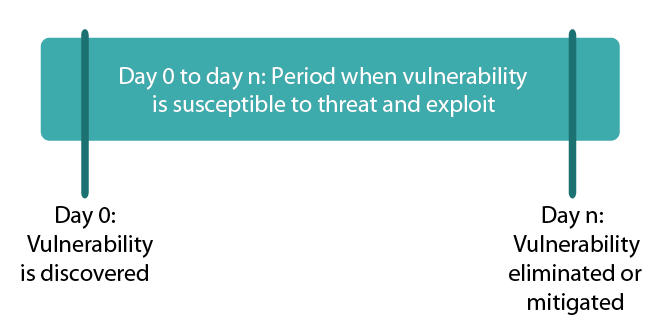
Vulnerability labels a condition or a set of conditions that create a weakness in systems or networks that can potentially be manipulated. Think of vulnerability as the susceptibility of a system or network to be attacked and possibly damaged or disrupted. Vulnerabilities take many forms:

* Easily guessable logon passwords
* Poorly configured access controls
* Exploitable programming flaws
* Incorrect security implementations
* Non-exploitable disruptive design flaws, such as denial of service (DoS)
* Undocumented maintenance or debugging backdoors in software or systems

All of these problems and many others can exist simultaneously across numerous systems and devices.

Threats, risks, and vulnerabilities negatively impact the confidentiality, integrity, and availability (C-I-A) triad. Confidentiality is breached when an attacker discloses private information, integrity is broken when an attacker modifies privileged data, and availability is ruined when an attacker successfully denies service to a mission-critical resource.

The length of time these vulnerabilities are present creates a window of vulnerability (WoV), the period within which defensive measures are reduced, compromised, or lacking. The WoV is the gap in time a workstation is exposed to a known vulnerability until it is patched. It also includes the time taken to create, publish, and finally apply a fix to the vulnerability. Problems arise as fixes can be disruptive to business operations and the delay between discovering and patching a hole leaves sufficient time for an attacker to intrude.



At any given time, a system or network will potentially have several overlapping WoVs, not all of which may be immediately identified. Remember, not all vulnerabilities are exploitable. Some exploits cause disruption such as DoS, while others may expose sensitive information or allow an attacker to take control.