# Software security lifecycle and security assessments

## Summary

In this class exercise, we will discuss the software security lifecycle, security assessments, and when security assessments should occur in the lifecycle. This should be performed without the aid of any electronic device.

## Prerequisites

* None

## Details

* Consider the phases in the product lifecycle below and their effects on the rows that describe them. For the column identified for your group, describe that phase in the product lifecycle using the concept from each row. E.g., is there high-, average-, or low-product usage by consumers in the phase-out phase?



Figure -Product lifecycle phases (ANSI/EIA-724)

| **Sales** | **Introduction** | **Growth** | **Maturity** | **Saturation** | **Decline** | **Phase-out** |
| --- | --- | --- | --- | --- | --- | --- |
| **Usage by consumers** |  |  |  |  |  |  |
| **External security assessment activity** |  |  |  |  |  |  |
| **Feature growth** |  |  |  |  |  |  |
| **Maker’s security process state** |  |  |  |  |  |  |
| **Support level** |  |  |  |  |  |  |
| **Sales** |  |  |  |  |  |  |

Figure -Notional stage summaries

* Discuss the software security lifecycle and its release cycles illustrated below amongst your group (note, these could occur in any product lifecycle phase). When would security assessments occur?

|  |  |
| --- | --- |
|  |  |
| Software security lifecycle | Software release cycles |

* Discuss the software vulnerability states illustrated below amongst your group. Label them in the areas provided in the SSL graphic on the right.

|  |  |
| --- | --- |
|  |  |
| Software vulnerability states | Vulnerability states in the software security lifecycle |

* Consider the figure below and discuss what occurs in a security assessment amongst your group. Write down an activity for each area. What is knowledge management in the context of a security assessment and why is it important?

|  |  |  |
| --- | --- | --- |
|  | Prepare |  |
| Step 1 |  |
| Step 2 |  |
| Step 3 |  |
| Step 4 |  |
| Step 5 |  |
| Step 6 |  |
| Knowledge management |  |
| Iterative software security assessment process |  | |

### Definitions

* Vulnerability-“Instance of a mistake in the specification, development, or configuration of software such that its execution can violate the explicit or implicit security policy” (Ozment 2007, 6-11; Krsul 1998)
* Exploit-Software threat that takes advantage of an existing vulnerability in order to compromise system or user assets
* Malware-Malicious software that generally performs something undesirable to system or user assets