**Respond**

* In here, basically it takes the appropriate actions for the detected cyber security events.
* This particular core function consists with multiple sub-categories as following.

1. Response Planning
2. Communications
3. Analysis
4. Mitigation
5. Improvements

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Sub Function** | **Description** | **Readiness** | | | |
| **Informal** | **Under Development** | **Already Established** | **Not Defined** |
| **Response Planning** | **Execute a response plan during or after a detected cyber event.** |  |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Sub Function** | **Description** | **Readiness** | | | |
| **Informal** | **Under Development** | **Already Established** | **Not Defined** |
| **Communications** | **Personnel training regarding roles and order of operations.** |  |  |  |  |
| **Reporting of events according to established criteria.** |  |  |  |  |
| **Sharing information in accordance with response plans.** |  |  |  |  |
| **Stakeholder coordination to ensure execution of response plans.** |  |  |  |  |
| **Voluntary information sharing with external stakeholders for broad cybersecurity awareness.** |  |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Sub Function** | **Description** | **Readiness** | | | |
| **Informal** | **Under Development** | **Already Established** | **Not Defined** |
| **Analysis** | **Investigate notifications from detection systems.** |  |  |  |  |
| **Understand the impact of an incident.** |  |  |  |  |
| **Perform forensics.** |  |  |  |  |
| **Categorize incidents in accordance with response plans.** |  |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Sub Function** | **Description** | **Readiness** | | | |
| **Informal** | **Under Development** | **Already Established** | **Not Defined** |
| **Mitigation** | **Contain events.** |  |  |  |  |
| **Mitigate events.** |  |  |  |  |
| **Mitigate or document the acceptance of risks for newly identified vulnerabilities.** |  |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Sub Function** | **Description** | **Readiness** | | | |
| **Informal** | **Under Development** | **Already Established** | **Not Defined** |
| **Improvements** | **Incorporate lessons learned.** |  |  |  |  |
| **Are updated regularly to meet the needs of a changing cyber landscape.** |  |  |  |  |