**Detect**

* In here, basically it makes the awareness within the organization about the cyber security events that may occur.
* This particular core function consists with multiple sub-categories as following.

1. Anomalies & Events
2. Security Continuous Monitoring
3. Detection Processes

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Sub Function** | **Description** | **Readiness** | | | |
| **Informal** | **Under Development** | **Already Established** | **Not Defined** |
| **Anomalies & Events** | **Establish and manage baseline network operations and data flows for users and systems.** |  |  |  |  |
| **Analyze detected events to understand attack targets and methods.** |  |  |  |  |
| **Combine data from events and link to multiple sources.** |  |  |  |  |
| **Determine impact of events.** |  |  |  |  |
| **Establish incident alert levels.** |  |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Sub Function** | **Description** | **Readiness** | | | |
| **Informal** | **Under Development** | **Already Established** | **Not Defined** |
| **Security Continuous Monitoring** | **The network to detect cybersecurity events.** |  |  |  |  |
| **The physical environment to detect cybersecurity events.** |  |  |  |  |
| **Personnel activity to detect cybersecurity events.** |  |  |  |  |
| **For malicious code.** |  |  |  |  |
| **For unauthorized mobile code.** |  |  |  |  |
| **External service provider activity to detect cybersecurity events.** |  |  |  |  |
| **Access by unauthorized personnel, connections, devices, and software.** |  |  |  |  |
| **System vulnerability by performing vulnerability scans.** |  |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Sub Function** | **Description** | **Readiness** | | | |
| **Informal** | **Under Development** | **Already Established** | **Not Defined** |
| **Detection Processes** | **Accountability for detection by having well-defined personnel roles and responsibilities.** |  |  |  |  |
| **Compliance with applicable organizational requirements for detection activities.** |  |  |  |  |
| **Testing of detection processes.** |  |  |  |  |
| **Communication of information pertaining to cyber events to appropriate parties.** |  |  |  |  |
| **Continuous improvement of detection processes.** |  |  |  |  |