#### 4.3 Detect Function

The Detect Function addresses the development and deployment of appropriate activities to monitor for anomalous events and notify downstream users and applications upon their occurrence. The Detect Function is informed by the Identify Function and is enabled by the Protect Function.

The objectives of the Detect Function include:

* Enabling detection through monitoring and consistency checking; and
* Establishing a process for deploying and handling detected anomalies and events.

The Detect Function defines three Categories, all of which have Subcategories that apply to SOC to varying degrees, as summarized in Sections 4.3.1 through 4.3.3.

##### 4.3.1 Anomalies and Events Category

Anomalous activity is detected, and the potential impact of events is understood. There are five Subcategories within Anomalies and Events all of which apply to the SOC.

# Table 14 - Anomalies and Events Subcategories

|  |  |  |
| --- | --- | --- |
| **Detect: Anomalies and Events**  **Subcategory**  **Applicability to the SOC** | | **References** |
| **DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed.** | Verify that operational performance baselines and expected data flows are captured, developed, and maintained to detect events.  When practical, comply with standards-based solutions for data formatting, message formatting, and message transmission to facilitate interoperability and integration. | **NIST SP 800-53 Rev. 5** AC-4, CA-3, CM-2, SC-16, SI-4 |
| **DE.AE-2: Detected events are analyzed to understand attack targets and methods.** | Review and analyze detected events within the SOC   1. real time to maintain normalcy of operations; and 2. forensically to understand the characteristics of anomalous events.   Be able to distinguish between potentially harmful events and normal operations and predict harm based on early indications and events.  Consider the SOC system when analyzing cybersecurity events involving space vehicles or other downstream systems.  For RFI, include environmental monitoring with direction-finding capabilities to locate the source.  Preserve the raw data, analysis, and characterization to aid in the analysis of future events. | **NIST SP 800-53 Rev. 5** AU-6, CA-7, IR-4, RA-5, SI-4  **RTCA 235** 2.1 |
| **DE.AE-3: Event data are collected and correlated from multiple sources and sensors** | Multiple sensors and sources can be used to correlate fault modes, cross check detected anomalies and contribute to anomaly detection models and algorithms.  Compile sufficient event data across the SOC using various sources, such as event reports, logs, audit monitoring, network monitoring, physical access monitoring, environmental monitoring, and HMI reports.  Standards-based data formatting and serialization promotes the communication interoperability and interchangeability of supporting data. | **NIST SP 800-53 Rev. 5** AU-6, CA-7, CP-2, IR-4, IR-5, IR-8, SI-4  **NIST SP 800-160 Rev. 1 3.3.7** Appendix G.2, G.3  **RTCA 235** 1.1 |
| **DE.AE-4: Impact of events is determined** | Identify the effects of anomalous events on the SOC itself and the corresponding space vehicle(s).  Events (including infrequent events and true anomalies) can have unexpected impacts on downstream devices and operations. | **NIST SP 800-53 Rev. 5** CP-2, IR-4, RA-3, SI-4 |
| **DE.AE-5: Incident alert thresholds are established** | Established incident thresholds with the understanding of potential impacts to the mission.  For critical applications, document error and uncertainty tolerances that serve as detection thresholds, which can be expressed as a statistical distribution within the confidence levels needed for operations. Consider and document the required notification or alarm communication time upon nearing and exceeding thresholds.  Consider reviewing and revising thresholds on a routine basis. | **NIST SP 800-53 Rev. 5** IR-4, IR-5, IR-8 |

##### 4.3.2 Security Continuous Monitoring Category

The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures. In the context of the SOC, the interface to the bus or payload, the receivers that process and form the commands, responses and telemetry, and the processed telemetry and state of health information from the space segment are monitored.

There are eight Subcategories within the Security Continuous Monitoring Category that apply to the SOC , as summarized in the table below.

# Table 15 - Security Continuous Monitoring Subcategories

|  |  |  |
| --- | --- | --- |
| **Detect: Security Continuous Monitoring**  **Subcategory**  **Applicability to the SOC** | | **References** |
| **DE.CM-1: The network is monitored to detect potential cybersecurity events** | Monitor network activity within the SOC as well as the bus and payload TT&C and compare against known baselines and expected reactions.  Heighten system monitoring activities when there is an indication of increased risk.  Fuse data from diverse sensors and probes. Consider using fault detection and exclusion algorithms to automatically detect faults and exclude erroneous sources in the analytics. This enables redundancy and consistency checking.  Verify that the monitoring strategy is sufficiently robust to detect space and ground segment behavior anomalies for all identified fault and failure modes. Detection thresholds should be determined from nominal and anomalous data for each fault and failure mode.  Detection models can leverage correlations between fault modes and minimum detectable limits. Analysis of the correlation engines may be able to determine if some faults can remain undetected. These findings can be used in the risk management procedures.  Software and hardware can be integrated into the SOC to detect and mitigate jamming and spoofing events in order to preserve data availability and integrity. | **NIST SP 800-53 Rev. 5** AU-12, CA-7,  CM3, SC-5, SC-7, SI-4  **RTCA 235** 2.3, 2.5 |
| **DE.CM-2: The physical environment is monitored to detect potential cybersecurity events** | Physical access to SOC is actively monitored to detect potential breaches in security.  Actively monitor the physical environment to include the RF environment.  SOC equipment such as antennas and alternate facilities may be in remote locations. Positively identify people who access these areas. Implement the use of access controls that are specific to personnel, such as biometrics, swipe cards and personal identification numbers (PINs). | **NIST SP 800-53 Rev. 5** CA-7, PE-6, PE-20 |
| **DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events** | Monitor personnel actions for unauthorized or atypical activity. The scope of the monitoring can include elements such as login attributes (e.g., time, physical location, operating system, device, credentials), electronic access control systems, physical access control systems (e.g., sign in/out sheets, logging), security status monitoring of personnel etc. | **NIST SP 800-53 Rev. 5** AC-2, AU-12, AU-13, CA-7, CM-10, CM-11 |
| **DE.CM-4: Malicious code is detected** | Given the importance of least functionality within the SOC, *all* code that is not in the baseline should be detected. | **NIST SP 800-53 Rev. 5** SC-44, SI-3, SI-4, SI-8 |
| **DE.CM-5: Unauthorized mobile code is detected** | Given the importance of least functionality, it is unlikely that SOC policy will permit any mobile code. | **NIST SP 800-53 Rev. 5** SC-18, SI-4, SC-44 |
| **DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events** | Not directly applicable to the SOC. SOCs responsible for the bus are typically stand alone networks. Commands sent to a hosted payload are cryptographically isolated from the bus, therefore only superficial monitoring is practical. | **NIST SP 800-53 Rev. 5** CA-7, PS-7, SA-4, SA-9, SI-4 |
| **DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed** | Directly applicable to the SOC to maintain least functionality and separation of duties. Monitor for system inventory discrepancies and conduct ongoing security status monitoring on SOC systems for unauthorized personnel, connections, devices, access points, and software. | **NIST SP 800-53 Rev. 5** AU-12, CA-7, CM-3, CM-8, PE-6, PE-20, SI-4 |
| **DE.CM-8: Vulnerability scans are performed** | Conduct vulnerability scans on SOC systems where safe, feasible, and in a manner that is consistent with industry best practices. Ensure that scanning activities do not negatively impact operations. | **NIST SP 800-53 Rev. 5** RA-5  **NIST SP 800-115** |

##### 4.3.3 Detection Processes Category

Detection processes and procedures are maintained and tested to ensure awareness of anomalous events. In the context of the SOC, the process and procedures on the information systems and assets as well as the analytic processes and procedures are maintained, updated, and tested.

There are five Subcategories within the Detection Process Category all of which apply to the SOC.

# Table 16 - Detection Processes

|  |  |  |
| --- | --- | --- |
| **Detect: Detection Processes**  **Subcategory**  **Applicability to the SOC** | | **References** |
| **DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability** | All roles including data collection, analytics, reporting and notification are identified and performance criteria defined. SOCs responsible for hosted payloads will require a collaborative arrangement with the host. | **NIST SP 800-53 Rev. 5** CA-2, CA-7, PM14 |
| **DE.DP-2: Detection activities comply with all applicable requirements** | Applicable to SOCs responsible for hosting third party payloads in accordance with pre-defined agreements. | **NIST SP 800-53 Rev. 5**, CA-1, CA-2, CA-7, PM-14, SI-1, SI-4, SR-1, SR-9, SR-10, all -1 controls |
| **DE.DP-3: Detection processes are tested** | Validate that event detection processes are operating as intended. SOC upgrades are re-validated with end-to-end testing by the users.  Perform periodic testing to verify the performance of the detection process against the most current threat profiles and vulnerabilities | **NIST SP 800-53 Rev. 5** CA-2, CA-7. PM-14, SI-3, SI-4 |
| **DE.DP-4: Event detection information is communicated** | Applicable to SOCs with buses that host (or SOCs with payloads that are hosted) by an independent organization. | **NIST SP 800-53 Rev. 5** AU-6, CA-2, CA-7, RA-5, SI-4 |
| **DE.DP-5: Detection processes are continuously improved** | Modify and improve the monitoring strategy as new fault modes are identified and until detection performance is acceptable.  Periodically examine the organization’s anomaly detection processes and seek improvements.  Re-evaluate the processes as the space segment ages to ensure sufficient robustness. | **NIST SP 800-53 Rev. 5** CA-2, CA-5, CA-7, PL-2, PM-14, RA-5, SI-4 |