4. Cyber Resilience Goal: ANTICIPATE | Cybersecurity function: DETECT

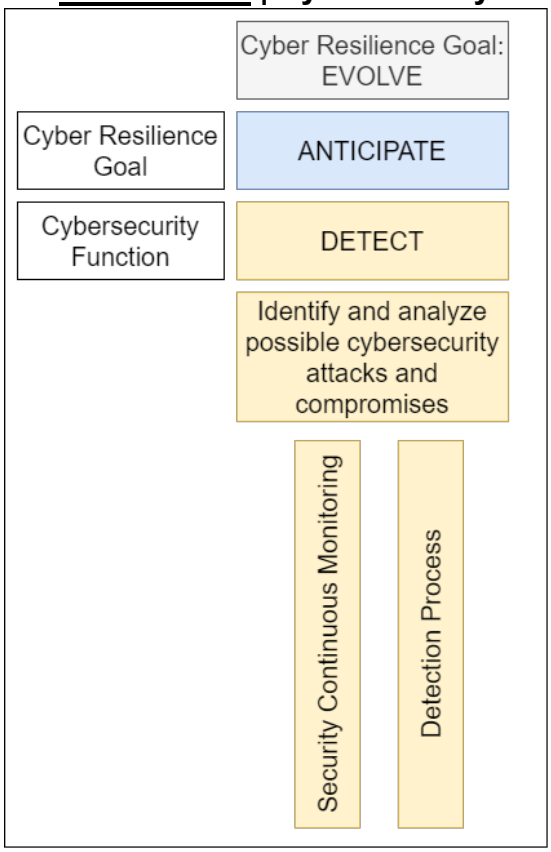

Figure 5: Overview of Detect function

4.1. DE.CM: Security Continuous Monitoring

i. DE.CM: Objective:

The REs' information systems and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.

ii. DE.CM: Standard:

1. The SOC shall cover (including but not limited to) network, endpoints, physical environment, personnel activities, malicious code, unauthorized mobile code, activities of third-party service providers, monitoring of unauthorized personnel, devices, connections and software, etc. Security Operations Centre (SOC)[20] shall be up and running 24×7×365 to monitor, prevent, predict, detect, investigate, and respond to cyber threats.
2. Appropriate continuous security monitoring mechanisms shall be established in SOC for the timely detection of anomalous or malicious activities.

[20] *SEBI through its circular CIR/MRD/CSC/148/2018 dated December 07, 2018 has mandated all stock exchanges, Clearing Corporations, and Depositories (except Commodities Derivatives Exchanges and their Clearing Corporation) to have a Cyber Security Operations Centre (C-SOC) that would be 24×7×365 set-up manned by dedicated security analysts to identify, respond, recover, and protect from cybersecurity incidents.*

3. All anomalies and alerts generated shall be properly monitored and investigated within stipulated time.
4. Capacity utilization shall be monitored for all the *critical systems* in the organization.
5. Cybersecurity audit, configuration audit, implementation audit, change management audit, and VAPT shall be conducted to detect vulnerabilities in IT environment.

Box Item 11: Security Operations Centre (SOC) and Market SOC

The key functions performed by SOC are as follows:

1. ***Continuous monitoring:*** *To monitor the end-points and network round the clock to immediately notify of abnormal or suspicious behavior.*

2. ***Log management:*** *To collect, maintain, and review logs of all end-points and network activities. Further, SOC aggregates and correlates data from various applications, firewalls, OS and endpoints to establish a baseline for normal behavior.*

3. ***Threat response:*** *To act as a first responder during a cybersecurity incident. Captive SOC is responsible to perform actions like isolating endpoints and limiting the damage with as little disruption of the business as possible. For all forms of managed SOC, the service provider shall alert the RE and guide them in incident management.*

4. ***Alert Management:*** *To monitor alerts issued by diverse tools and closely inspect each one of them in order to discard false positives (if any), and determine the potential impact of threats.*

5. ***Root Cause Investigation:*** *Post the occurrence of incident, SOC is responsible for investigating when, how and why an incident occurred. SOC analyzes all logs to identify the root cause of the incident and prevent its reoccurrence after incorporating learnings from the incident.*

While SOC serves twofold purpose, i.e., assessing and alerting security threats in real time thereby continuously improving organization's security posture, however, setting-up own SOC may be onerous for the small REs. Therefore, to improve the cybersecurity posture of such REs, CSCRF provides setting different types of SOC. CSCRF has mandated SOC for all REs (except client-based stock brokers having less than 100 clients). However, CSCRF allows REs to choose any one of the below models to utilize SOC services:

1. *RE's own/ group SOC*
2. *Market SOC implemented mandatorily by NSE, BSE and optionally by NSDL and/ or CDSL*
3. *Any other third-party managed SOC*

Small-Size and Self-certification category REs are mandated to be on-boarded on above-mentioned Market SOC.

SEBI's expectations from Market SOC are as follows:

1. *To provide cyber hygiene for Indian securities market ecosystem by providing cost-effective solutions.*
2. *For small-size and mid-size REs, Market SOC shall also provide services of VAPT and cyber audit at an affordable cost. Further, the above-mentioned VAPT and cyber audit should be conducted by a CERT-In empanelled IS Auditing Organization.*

The particulars of the Market SOC shall be as follows:

1. *The Market SOC shall be setup:*
   a. *Mandatorily by NSE and BSE*

b. Optionally by NSDL and/ or CDSL

2. *The Market SOC shall be set up in accordance with the CSCRF requirements and shall ensure that participating REs are in compliance with CSCRF as applicable to them.*
3. *The Market SOC shall bridge technological gap for small REs and provide them robust SOC services. However, the responsibility and accountability for compliance with CSCRF rests with the REs.*
4. *The Market SOC shall evolve continuously in order to incorporate new security controls and guidelines that may be issued by SEBI from time to time.*
5. *The Market SOC provider shall ensure that the REs participating in their SOC adhere to the minimum IT guidelines and security protocols all the time.*
6. *NSE and BSE (NSDL and CDSL, if applicable) shall carry out audit of their Market SOC activity annually and submit the report to SEBI.*

*Functional efficacy of market SOC shall be measured in accordance with **Annexure-N** of CSCRF and shall be reported along with market SOC providers' cyber audit report.*

4.2. DE.DP: Detection Process

i. DE.DP: Objective

Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.

ii. DE.DP: Standard

1. Roles and responsibilities for detection are defined to ensure accountability.
2. REs shall ensure that detection processes are tested by developing playbooks and use-cases.
3. Event detection information shall be communicated as per the regulatory requirements and organizational policies.
4. MIIs and Qualified REs shall conduct goal-based adversarial simulation red teaming exercise on a periodic basis to identify potential weaknesses within the organization's cyber defense.
5. REs shall conduct threat hunting and compromise assessment on a regular basis.