भारतीय प्रतिभूति और विनिमय बोर्ड
Securities and Exchange Board of India

CIRCULAR

CIR/MRD/CSC/148/2018 December 07, 2018

To,

All Stock Exchanges, Clearing Corporations and Depositories (except Commodities Derivatives Exchanges and their Clearing Corporations).

Dear Sir / Madam,

Cyber Security and Cyber Resilience framework of Stock Exchanges, Clearing Corporations and Depositories

1. Recognizing the need for a robust Cyber Security and Cyber Resilience framework at Market Infrastructure Institutions (MIIs), i.e., Stock Exchanges, Clearing Corporations and Depositories, vide SEBI Circular CIR/MRD/DP/13/2015 dated July 06, 2015, a detailed regulatory framework on cyber security and cyber resilience was prescribed.

2. With the view to further strengthening the aforesaid framework, particularly in respect of monitoring of cyber threats and cyber resiliency, the matter was discussed with SEBI's Technical Advisory Committee (TAC), SEBI's High Powered Committee on Cyber Security (HPSC-CS) and the MIIs.

3. Accordingly, it has been decided that MIIs shall have a Cyber Security Operation Center (C-SOC) that would be a *24x7x365* set-up manned by dedicated security analysts to identify, respond, recover and protect from cyber security incidents.

4. The C-SOC shall function in accordance with the framework specified in SEBI Circular CIR/MRD/DP/13/2015 dated July 06, 2015. Illustrative list of broad functions and objectives to be carried out by a C-SOC are mentioned hereunder:

   4.1. Prevention of cyber security incidents through proactive actions:

   (a) Continuous threat analysis,

   (b) Network and host scanning for vulnerabilities and breaches,

   (c) Countermeasure deployment coordination,

(d) Deploy adequate and appropriate technology at the perimeter to prevent attacks originating from external environment and internal controls to manage insider threats. MIIs may implement necessary controls to achieve zero trust security model.

4.2. Monitoring, detection, and analysis of potential intrusions / security incidents in real time and through historical trending on security-relevant data sources.

4.3. Response to confirmed incidents, by coordinating resources and directing use of timely and appropriate countermeasures.

4.4. Analysis of the intrusions / security incidents (including Forensic Analysis and Root Cause Analysis) and preservation of evidence.

4.5. Providing situational awareness and reporting on cyber security status, incidents, and trends in adversary behavior to appropriate organizations including to CERT-In and NCIIPC.

4.6. Engineer and operate network defense technologies such as Intrusion Detection Systems (IDSes) and data collection / analysis systems.

4.7. MIIs to adopt security automation and orchestration technologies in C-SOC to automate the incident identification, analysis and response as per the defined procedures.

5. Further to the above, the C-SOC of MII shall, at the minimum, undertake the following activities:

5.1. In order to detect intrusions / security incidents in real time, the C-SOC should monitor and analyze on a *24x7x365* basis relevant logs of MII's network devices, logs of MII's systems, data traffic, suitable cyber intelligence (intel) feeds sourced from reliable vendors, inputs received from other MIIs, inputs received from external agencies such as CERT-In, etc. The cyber intelligence (intel) feeds may include cyber news feeds, signature updates, incident reports, threat briefs, and vulnerability alerts.

5.2. To this end, appropriate alert mechanisms should be implemented including a comprehensive dashboard, tracking of key security metrics and provide for cyber threat scorecards.

5.3. The C-SOC should conduct continuous assessment of the threat landscape faced by the MII including undertaking periodic VAPT (Vulnerability Assessment and Penetration Testing).

5.4. The C-SOC should have the ability to perform Root Cause Analysis, Incident Investigation, Forensic Analysis, Malware Reverse Engineering, etc. to determine the nature of the attack and corrective and/or preventive actions to be taken thereof.

5.5. The C-SOC should conduct periodic (at the minimum quarterly) cyber attack simulation to aid in developing cyber resiliency measures. The C-SOC should develop and document mechanisms and standard operating procedures to recover from the cyber-attacks within the stipulated RTO of the MII. The C-SOC should also document various scenarios and standard operating procedures for resuming operations from Disaster Recovery (DR) site of MII.

5.6. The C-SOC should conduct periodic awareness and training programs at the MII and for its members / participants / intermediaries with regard to cyber security, situational awareness and social engineering.

5.7. The C-SOC should be capable to prevent attacks similar to those already faced. The C-SOC should also deploy multiple honey pot services which are dynamic in characteristics to avoid being detected as honey *pot* by attackers.

6. As building an effective C-SOC requires appropriate mix of right people, suitable security products (Technology), and well-defined processes and procedures (Processes), an indicative list of areas that MIIs should consider while designing and implementing a C-SOC are as follows:

6.1. The MII shall ensure that the governance and reporting structure of the C-SOC is commensurate with the risk and threat landscape of the MII. The C-SOC shall be headed by the Chief Information Security Officer (CISO) of the MII. The CISO shall be designated as a Key Managerial Personnel (KMP) and relevant provisions relating to KMPs in the *SEBI Securities Contracts (Regulation) (Stock Exchanges and Clearing Corporations) Regulations, 2012* and the subsequent circulars issued by SEBI relating to KMPs, shall apply to the CISO.

6.2. While the CISO is expected to work closely with various departments of MIIs, including MII's Network team, Cyber Security team and Information Technology (IT) team, etc., the reporting of CISO shall be directly to the MD & CEO of the MII.

6.3. The roles and responsibilities of CISO may be drawn from Ministry of Electronics and IT notification No. 6(12)/2017-PDP-CERT-In dated March 14, 2017.

6.4. The C-SOC should deploy appropriate technology tools of adequate capacity to cater to its requirements. Such tools shall, at the minimum, include Security

Analytics Engine, Malware detection tools, Network and User Traffic Monitoring and Behavior Analysis systems, Predictive Threat Modelling tools, Tools for monitoring of System parameters for critical systems / servers, Deep Packet Inspection tools, Forensic Analysis tools, etc.

6.5. Each MII is advised to formulate a Cyber Crisis Management Plan (CCMP) based on its architecture deployed, threats faced and nature of operations. The CCMP should define the various cyber events, incidents and crisis faced by the MII, the extant cyber threat landscape, the cyber resilience envisaged, incident prevention, cyber crisis recognition, mitigation and management plan. The CCMP should be approved by the respective Standing Committee on Technology / IT-Strategy Committee of the MIIs and the governing board of the MII. The CCMP should also be reviewed and updated annually.

6.6. The C-SOC should have well-defined and documented processes for monitoring of its systems and networks, analysis of cyber security threats and potential intrusions / security incidents, usage of appropriate technology tools deployed by C-SOC, classification of threats and attacks, escalation hierarchy of incidents, response to threats and breaches, and reporting (internal and external) of the incidents.

6.7. The C-SOC should employ domain experts in the field of cyber security and resilience, network security, data security, end-point security, etc.

6.8. The MIIs are also advised to build a contingent C-SOC at their respective DR sites with identical capabilities w.r.t. the primary C-SOC in line with the SEBI Circular CIR/MRD/DMS/12/2012 dated April 13, 2012 read with SEBI Circular CIR/MRD/DMS/17/2012 dated June 22, 2012. Additionally, the MIIs should perform monthly live-operations from their DR-C-SOC.

6.9. The C-SOC should document the cases and escalation matrices for declaring a disaster.

7. In view of the feedback received from MIIs, it has been decided that MIIs may choose any of the following models to set-up their C-SOC :

   (i) MII's own C-SOC manned primarily by its internal staff,

   (ii) MII's own C-SOC, staffed by a service provider, but supervised by a full time staff of the MII. (Refer to 7.3)

   (iii) C-SOC that may be shared by the MII with its group entities (that are also SEBI recognized MIIs),

(iv) C-SOC that may be shared by the MII with other SEBI recognized MII(s).

7.1. The responsibility of cyber security of an MII, adherence to business continuity and recovery objectives, etc. should lie with the respective MII, irrespective of the model adopted for C-SOC.

7.2. The respective risk committee(s) of the MII should evaluate the risks of outsourcing the respective activity.

7.3. The MII may outsource C-SOC activities in line with the guidelines as given in Annexure-A.

8. A report on the functioning of the C-SOC, including details of cyber-attacks faced by the MII, major cyber events warded off by the MII, cyber security breaches, data breaches should be placed on a quarterly basis before the board of the MII.

9. The system auditor of the MII shall audit the implementation of the aforesaid guidance in the annual system audit of the MII. The Scope and/or Terms of Reference (ToR) of the annual system would accordingly be modified to include audit of the implementation of the aforementioned areas.

10. Further, in continuation to the requirement specified at para 52 of the Annexure A to the aforementioned SEBI Circular dated July 06, 2015, the C-SOC shall share relevant alerts and attack information with members / participants / intermediaries of the MII, other MIIs, external cyber response agencies such as CERT-In, and SEBI.

11. MIIs are directed to take necessary steps to put in place appropriate systems and processes for implementation of the circular, including necessary amendments to the relevant bye-laws, rules and regulations, if any, within six months from the date of the circular. In case wherein a MII currently has a C-SOC set-up that is different from that mentioned at para 7(i) - 7(iv), such MIIs are directed to adopt and transit to one of the models mentioned at para 7(i) - 7(iv) within a period of one year from the date of issuance of this circular.

12. This circular is being issued in exercise of powers conferred under Section 11 (1) of the Securities and Exchange Board of India Act, 1992 and Section 19 of the Depositories Act, 1996 to protect the interests of investors in securities and to promote the development of, and to regulate the securities market.

Yours faithfully,

Bithin Mahanta

Deputy General Manager
Cyber Security Cell
Market Regulation Department
Email: bithinm@sebi.gov.in

Annexure A

1. Level of support definitions for outsourcing/in-house are as follows:

    1.1. Security Analyst Level 1 (L1): This function may be mostly outsourced

    (a) Monitoring SIEM Solution console for identifying the security events generated by the log sources integrated with SIEM tools.

    (b) Identification of security events that are false +ve before qualifying event as an incident.

    (c) Identify the exceptions which are identified as an event (e.g. VA scanning performed by SEBI appointed 3rd party which may be identified as port scanning attack) .

    (d) Perform first level event analysis before qualifying the incidents.

    (e) Qualifying the event as an incident using Knowledgebase.

    (f) Escalating exceptions & Events to L2 level.

    (g) Log Incident tickets in service management tool and assign it to the respective team.

    (h) Follow-up for the closure of the incident tickets generated.

    1.2. Security Analyst Level 2 (L2): Combination of Outsource / In-House

    (a) Exception Analysis.

    (b) Analysis of extended events.

    (c) Confirmation of False +ve & update Knowledge Base.

    (d) Qualify Incident & provide mitigation suggestions.

    (e) Escalate incident to next level.

    (f) Update /configuration correlation rules after approval.

    1.3. Security Analyst Level 3 (L3): Combination of Outsource / In-House

    (a) Analysis of escalated Incidents.

    (b) Define correlation rules.

(c) Analysis of impact on SIEM over all correlation rules and operations for the correlation rules suggested by Level 2 Analyst.

(d) Approve correlation rules after the impact analysis.

(e) Perform impact analysis before deployment of correlation rules.

(f) Perform impact analysis for update and upgrade of SIEM & Advance security solutions components.

(g) Define Mitigation suggestions for newly identified incidents.

(h) Approve the reports before sharing with others.

1.4. SOC Manager (L4) : In-house

(a) Lead and manage Security Operations Centre.

(b) Provide strategic directions to SOC team and organization for security posture improvements.

(c) To identify key contacts for incident escalation and change management activities.

(d) Ensure compliance to SLA.

(e) Ensure process adherence and process improvisation to achieve operational objectives.

(f) Revise and develop processes to strengthen the current Security Operations.

(g) Responsible for team and vendor management.

(h) Responsible for overall use of resources and initiation of corrective action where required for Security Operations Center.

(i) Escalate to the other IT Infra. Management teams or application maintenance teams, as necessary.

(j) Overall responsibility for delivery of in scope activities as a part of this engagement.

(k) Point of contact for problem escalation and reporting.

1.5. Security Subject Matter Expert for Security technologies: In-house with reliance on external expertise

(a) Subject Matter Expert (SME) for SIEM and Advance security solutions.

(b) Assist you with troubleshooting steps to be performed by you in order to re-establish connectivity between the SIEM System and SEBI's locations.

(c) Provide software-level management for the SIEM System components;

(d) Verify data collection and log continuity;

(e) Manage user access including user and group permissions updates;

(f) Review application performance, capacity, and availability make recommendations as appropriate;

(g) Review SIEM System disk space usage;

(h) Verify time synchronization among SIEM System components;

(i) Perform archival management and retrieval per change management process;

(j) Provide problem determination / problem source identification for the SIEM System, consisting of creating tickets & tracking progress of Open tickets

(k) Managing tickets to resolution / closure, in accordance with the processes as defined in the Integrated and Transition vendor announcements & manage SIEM System update alerts;

(l) Install application patches and software updates in order to improve performance, or enable additional functionality

Illustrative Training Requirements

Security Analyst Level 1 (L1):

1) SEC401: Security Essentials Bootcamp Style
https://www.sans.org/event/cyber-defence-canberra-2018/course/security-essentials-bootcamp-style

2) SEC301: Introduction to Cyber Security
https://www.sans.org/course/introduction-cyber-security

Security Analyst Level 2 (L2):

1) SEC542: Web App Penetration Testing and Ethical Hacking
https://www.sans.org/event/cyber-defence-canberra-2018/course/web-app-penetration-testing-ethical-hacking

2) SEC566: Implementing and Auditing the Critical Security Controls - In-Depth
https://www.sans.org/private-training/course/implementing-auditing-critical-security-controls

3) SEC575: Mobile Device Security and Ethical Hacking
https://www.sans.org/private-training/course/mobile-device-security-ethical-hacking

Security Analyst Level 3 (L3):

1) SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling
https://www.sans.org/event/cyber-defence-canberra-2018/course/hacker-techniques-exploits-incident-handling

2) FOR508: Advanced Digital Forensics, Incident Response, and Threat Hunting
https://www.sans.org/event/digital-forensics-summit-2018/course/advanced-incident-response-threat-hunting-training

3) SEC501: Advanced Security Essentials - Enterprise Defender
https://www.sans.org/private-training/course/advanced-security-essentials-enterprise-defender

4) MGT414: SANS Training Program for CISSP® Certification
https://www.sans.org/course/sans-plus-s-training-program-cissp-certification-exam

SOC Manager (L4):

1) Cyber Security Specialist
http://www.leaderquestonline.com/it-career-training/cybersecurity-specialist/

2) Managing Security Operations: Detection, Response, and Intelligence
https://www.sans.org/event/rocky-mountain-2018/course/managing-security-operations-detection-response-and-intelligence

3) SIEM with Tactical Analytics
https://www.sans.org/private-training/course/siem-with-tactical-analytics

4) SEC511: Continuous Monitoring and Security Operations
https://www.sans.org/course/continuous-monitoring-security-operations

5) SEC599: Defeating Advanced Adversaries - Implementing Kill Chain Defenses
https://www.sans.org/course/defeating-advanced-adversaries-kill-chain-defenses