AUJAS CYBERSECURITY
A NuSummit Company

M-SOC Workshop
NSE Market SOC (M-SOC) Offerings as per CSCRF

Partnered with Aujas Cybersecurity Limited

AUJAS CYBERSECURITY

A NuSummit Company

NSE - Market SOC

Executive Summary

AUJAS CYBERSECURITY
A NuSummit Company

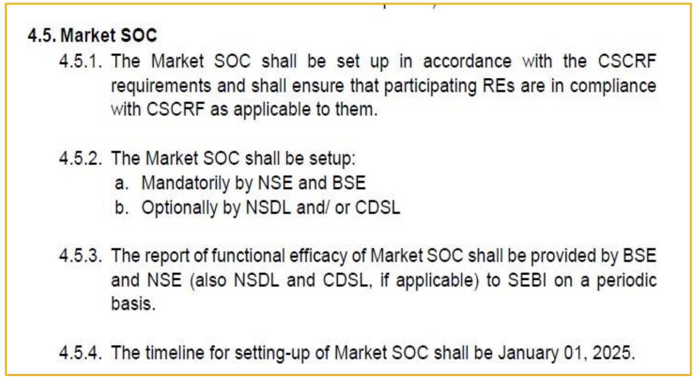
NSE Market SOC (M-SOC) powered by Aujas is a cybersecurity solutions provider for smaller entities that may not have the resources to set up their own Security Operation Centre (SOC). The M-SOC is run by the National Stock Exchange (NSE) and the Bombay Stock Exchange (BSE). The Securities and Exchange Board of India (SEBI) released a cybersecurity framework in **August 2024** that requires all registered entities to establish a SOC.

The framework follows a graded approach and classifies the REs in the following five categories based on their span of operations and certain thresholds like number of clients, trade volume, asset under management, etc.:

- Market Infrastructure Institutions (MIIs)
- Qualified REs
- Mid-size REs
- Small-size REs
- Self-certification REs

The framework mandates the establishment of SOCs and the development of the Cyber Capability Index (CCI). The framework is intended to help maintain market integrity and stakeholder trust. The framework provides cybersecurity solutions tailored to the needs of small entities.

This Deck provides the M-SOC services provided by NSE in Partnership with Aujas Cyber Security. These services cover comprehensively; all the aspects of M-SOC and provides budget friendly services to those REs who cannot implement their own SOC or give individual third party SOC (TP- SOC) contracts



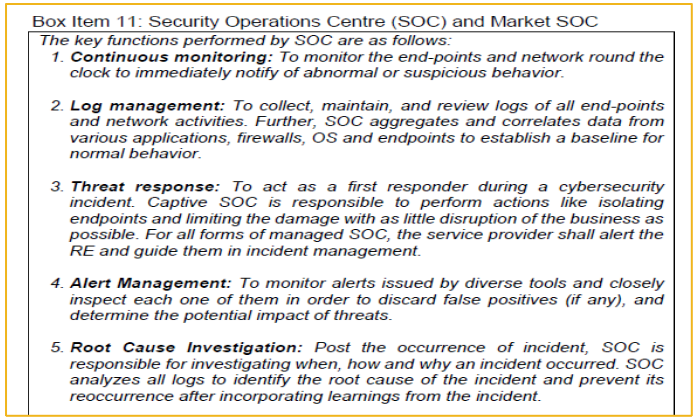
4.5. Market SOC

4.5.1. 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.

4.5.2. The Market SOC shall be setup:
a. Mandatorily by NSE and BSE
b. Optionally by NSDL and/ or CDSL

4.5.3. The report of functional efficacy of Market SOC shall be provided by BSE and NSE (also NSDL and CDSL, if applicable) to SEBI on a periodic basis.

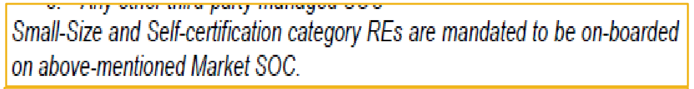
4.5.4. The timeline for setting-up of Market SOC shall be January 01, 2025.



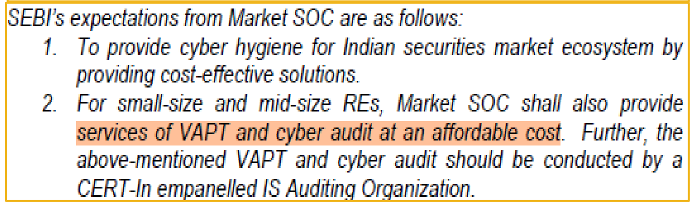
Box Item 11: Security Operations Centre (SOC) and Market SOC

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.*



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

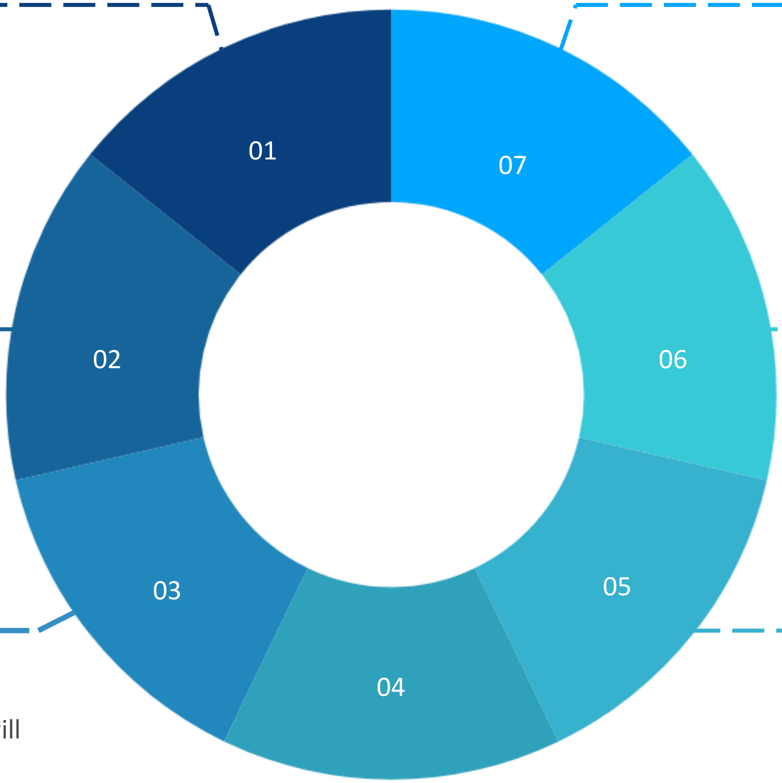


SEBI's expectations from Market SOC are as follows:

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.*

MSOC Scope of services

AUJAS CYBERSECURITY
A NuSummit Company



24x7 Monitoring (Logs & EDR)

24x7 monitoring of RE endpoint security logs. Qualified Security Analysts review and escalate incidents. EDR Agent is optional. REs may use any EDR agent of their choice.

Incident Management

MSOC to share Incident Management Process with all RE(s).

Native Case Mgmt.

Native built-in Case Management allow RE(s) to view and manage incidents. Regulator/auditors will have access to cases.

Centralized Dashboarding/Report

Ongoing deliverables/KPIs dashboarding and reporting

Log Retention & Compliance Reports

Six (6) months Online, and Eighteen (18) months offline (Optional) .

Weekly & Monthly automated reports.

Multi- Tenancy

RE(s) can view only their data. Regulators and auditors can view and monitor all RE(s) cases and data for compliance.

Threat Intelligence

Threat Intelligence from multiple sources including CERT-IN and NCIIPC

Aujas M-SOC Services for Self-certified REs

All Aujas Market SOC Pricing Tiers comply with the CSCRF SOC Guidelines which are narrated to the right side

Services	0-100 EPS	Upto 200 EPS	Upto 300 EPS	Upto 400 EPS	Upto 500 EPS
EDR MSSP with Services	✓	✓	✓	✓	✓
SIEM Licenses	✓	✓	✓	✓	✓
SIEM Implementation	✓	✓	✓	✓	✓
SIEM Administration	✓	✓	✓	✓	✓
Use Cases Creation	✓	✓	✓	✓	✓
Dashboards and Reports	✓	✓	✓	✓	✓
24*7 CDC Monitoring	✓	✓	✓	✓	✓
1 Custom App Integration				✓	✓

Monitoring the Detection

- Continuous Security Monitoring
- Functional Efficacy Assessments and Reporting with Bi-Annual to One year assessment frequency

Compliance and Reporting

- Incident Reporting in the Prescribed Reporting Format
- Market SOC Reporting

Adoption Timeline

- 1st Jan 2025: For REs who are Previously Covered by earlier SEBI Circulars
- 1st Apr 2025: Other REs under the new CSCRF Guidelines

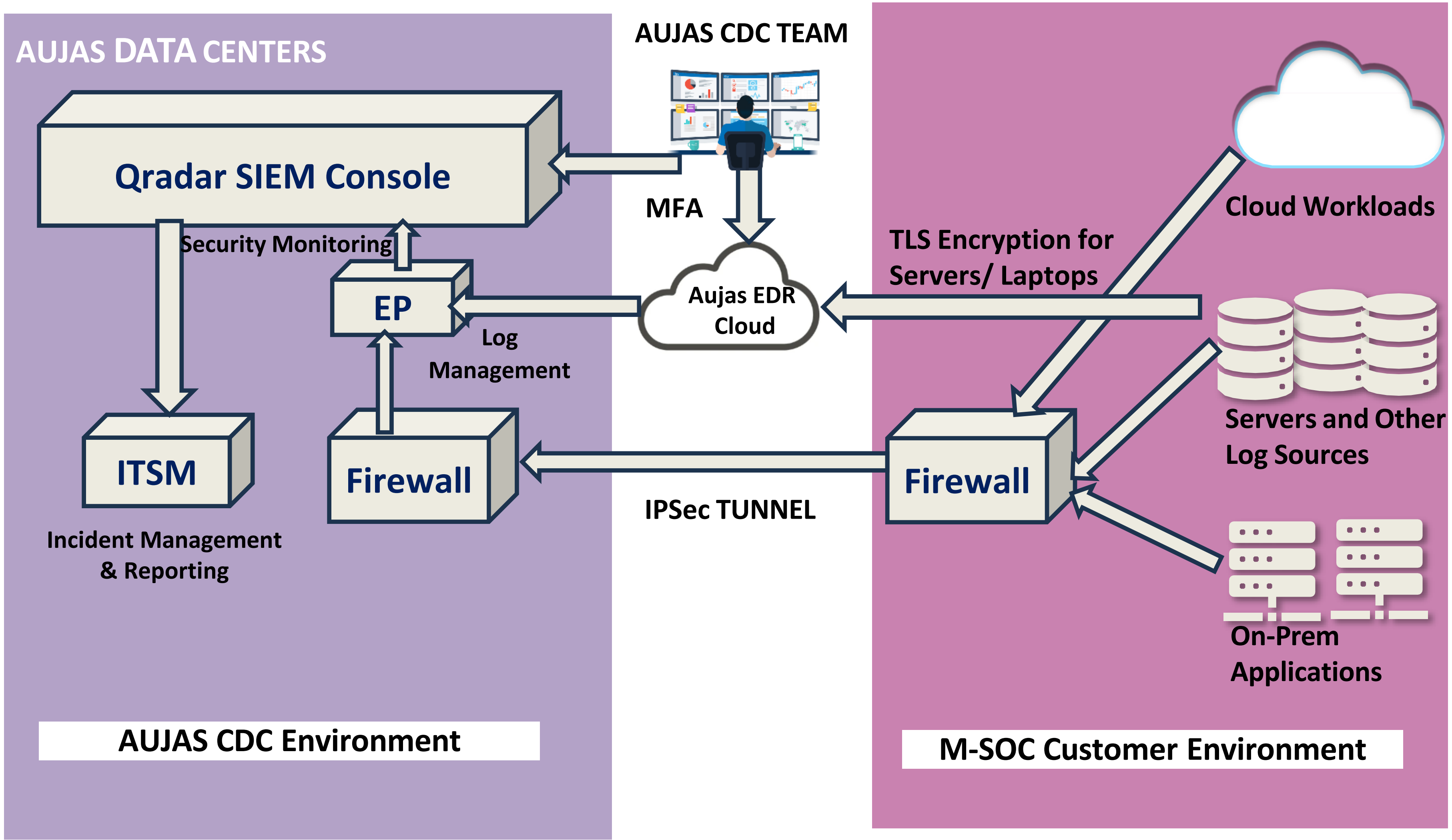
NSE M-SOC Services Scope

NSE Market SOC as per SEBI CSCRF circular has to cover the below mentioned SOW for self-certified, small and mid size regulated entities. We have further segregated RE by avg. estimated EPS consumption. We will be able to on board RE from a base of 5-8 devices upto 100EPS PA for M-SOC. The no. of devices to be covered in M-SOC shall be provided by the RE, client has to share the asset inventory that need to be integrated with SIEM, based on the asset inventory EPS will be calculated.

Please check below, the segmentation of M-SOC SOW for RE:

MSOC Services/RE’s	SELF-CERTIFICATION	SMALL	MID-SIZE
EDR MSSP with Services	✓	✓	✓
SIEM Licenses	✓	✓	✓
SIEM Implementation	✓	✓	✓
SIEM Administration	✓	✓	✓
Use Cases Creation	✓	✓	✓
Dashboards and Reports	✓	✓	✓
24*7 CDC Monitoring	✓	✓	✓
Log storage 6 months online and 18 months offline	✓	✓	✓

M-SOC Sample Architecture – Module 1

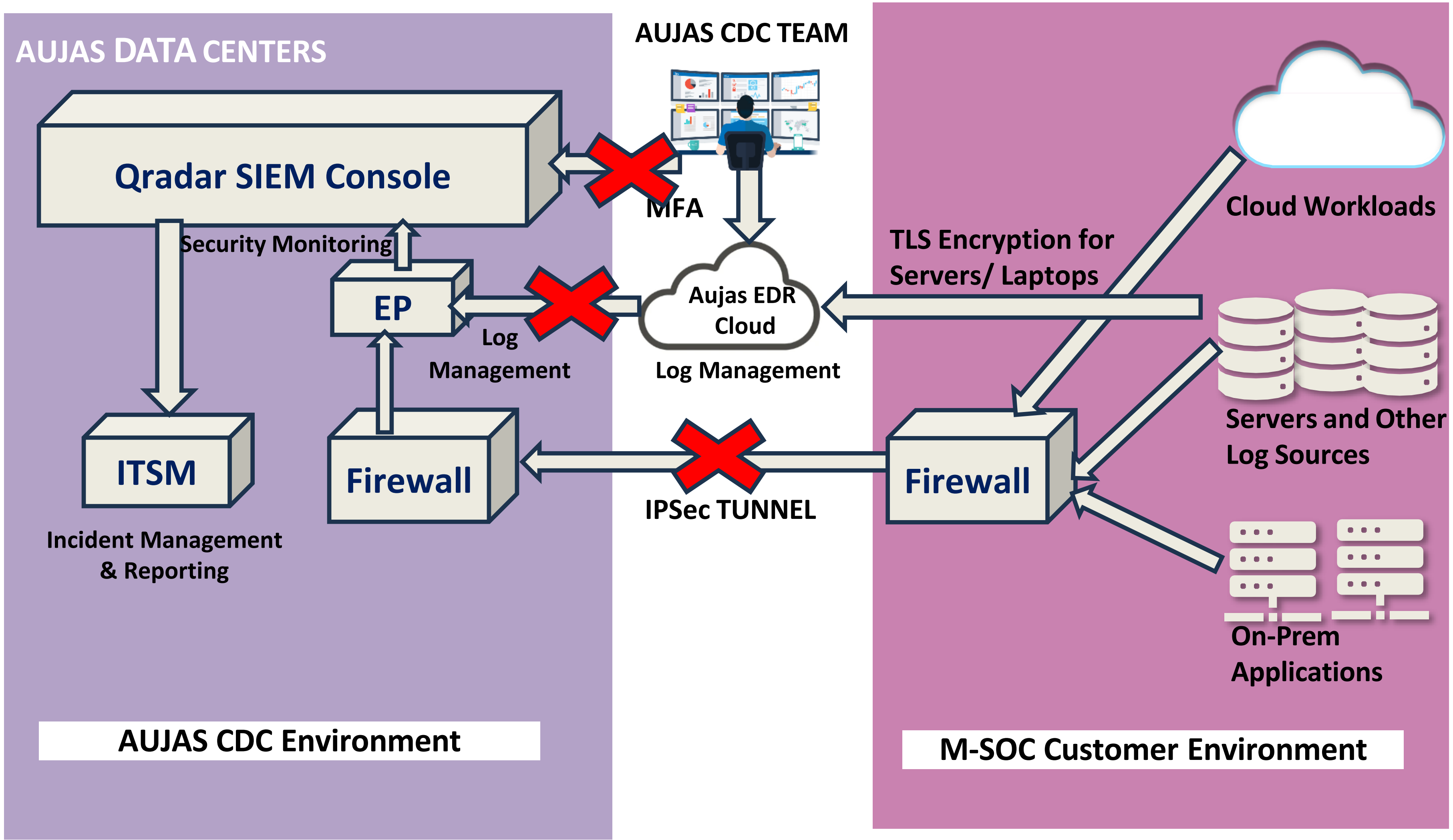


MFA – Multi-Factor Authentication, EP – Event Processor, ITSM – IT Service Management, TLS – Transport Layer Security, M-SOC – Market SOC, EDR – Endpoint Detection and Response, SIEM – Security Information and Event Management, CDC – Cyber Defense Center, IPSec – IP Security

- Further Customizable on case-to-case basis
- Logs will remain in Aujas EP
- MSSP Services from Aujas CDCs
- Optional access on the ITSM for customer

- SLA Driven; Outcome based services
- Implementation Time between 2-8 weeks depending on size of RE

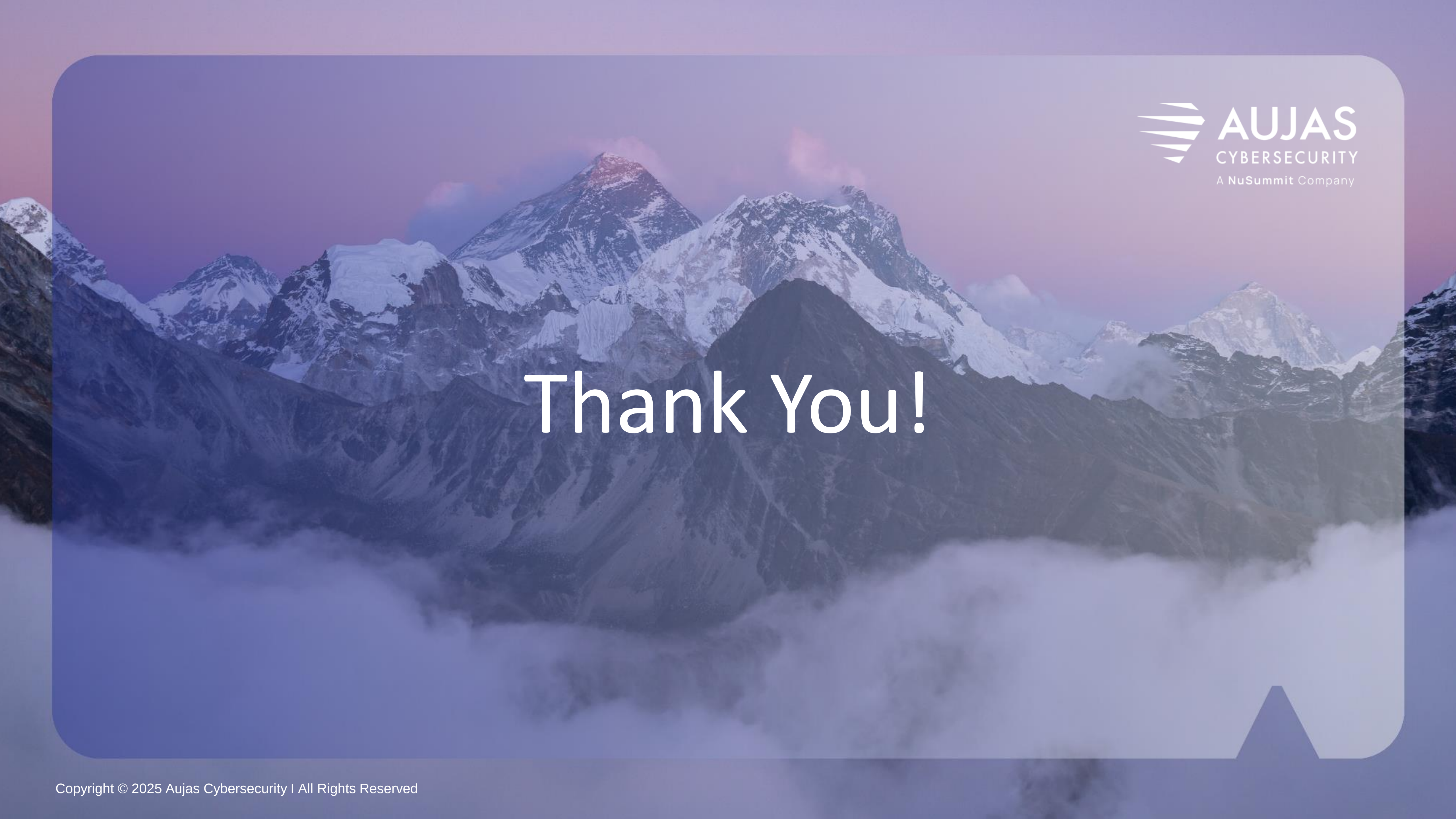
M-SOC Sample Architecture – Module 2



- Further Customizable on case-to-case basis
- Logs will remain in Aujas EP
- MSSP Services from Aujas CDCs
- Optional access on the ITSM for customer

- SLA Driven; Outcome based services
- Implementation Time between 2-8 weeks depending on size of RE

MFA – Multi-Factor Authentication, EP – Event Processor, ITSM – IT Service Management, TLS – Transport Layer Security, M-SOC – SOC, EDR – Endpoint Detection and Response, SIEM – Security Information and Event Management, CDC – Cyber DefensMarkCenterete, IPSec – IP Security



Thank You!