Expression of Interest

Selection of Business Partners

For

Planning and execution of Hindustan Zinc cyber security program cum roadmap to have cyber-resilience

Date – 3 February 2025

Hindustan Zinc Limited

Phone +91 294-6604000

Website www.hzlindia.com

Yashad Bhawan,

Udaipur–313 004,

Rajasthan, INDIA.

Introduction

Hindustan Zinc Limited (HZL) is the world's second largest integrated zinc-lead-silver producer and India's only vertically integrated zinc-lead-silver producer. HZL is a subsidiary of Vedanta Limited, a globally diversified natural resources company. The company has its headquarters in Udaipur, Rajasthan, India.

In-Scope entities:
Head office – Udaipur, Rajasthan

(Other operational locations):
Smelters & refineries

- Debari
- Dariba
- Chanderiya
- Pantnagar

Mines

- Rampura Agucha
- Sindesar Khurd
- Rajpura Dariba
- Zawar
- Kayad

Technical Scope of work

HZL is seeking a globally reputed consultancy agency for the following scope of work:

1. Define acceptable risk level and perform a cyber risk assessment to identify potential high-risk areas; create a mitigation plan to bring down risk to acceptable level.
2. Perform a capability maturity assessment and benchmarking to identify where HZL stands in comparison to its global and Indian peers
3. Take inputs from both above and create strategic roadmap for cyber security program at Hindustan Zinc with the goal to achieve cyber-resilience
4. Define KPIs and executive dashboards to track health and progress
5. Some of the representative security platforms/technologies that are planned to be implemented are enumerated as below (subject to change depending on the recommendation of the selected agency):
    a. Cloud native application protection platform (CNAPP)
    b. Secure service edge (SSE) including ZTNA (Zero Trust Network) and CASB (Cloud access security broker)
    c. Network access control (NAC)
    d. Data security posture management (DSPM)
    e. Database classification, encryption and masking
    f. Intelligent/Automated Data Classification
    g. Consent management platform

h. CPS protection platform comprising OT SIEM, Asset discovery, Vulnerability Assessment, Remote Access platform
i. Implementation of OT SOC
j. IGA (Identity Governance and Administration)
k. API Security

6. Interdependent technology landscape of other Vedanta entities needs to be taken into consideration while implementing these security platforms
7. Assist in evaluation of security platforms identified as part of the roadmap exercise, and handle Project Management Office (PMO) for implementation of the said platforms.
8. Perform vulnerability assessment, penetration testing, configuration review, code review and rule-base review of HZL IT infrastructure including SAP applications (to commence from 1st July 2025) and assist in remediation and perform revalidation to ensure closure by coordinating with various IT/Vendor SPOCs both in HZL and at Vedanta Corp. Scope is as below:
   a. Security assessment of ~100 Web/mobile app plus any new applications getting deployed) (Assessment of 30 critical apps every year, and rest of the apps to be staggered over 3 years)
   b. Security assessment of all APIs used by in-scope web and mobile apps
   c. Security assessment of ~240 Servers comprising Windows and Unix/Linux plus any new servers getting commissioned every year
   d. Security assessment of ~40 Databases comprising SQL and Oracle, plus any new databases getting commissioned every year
   e. Security assessment of 11 IT perimeter firewalls and 21 OT firewalls, plus any new firewalls getting commissioned every year
   f. Security assessment of ~700Network devices such as switches, access points, wireless controllers (50 critical network devices every year, and rest of the network devices staggered over 3 years)
   g. Security assessment of Active Directory (4 servers)
   h. Security assessment of ~3000 Endpoints (laptops, desktops, workstations) by taking 10% sample endpoints every year
   i. Security assessment of Azure and GCP Cloud (all HZL assets and supporting infrastructure hosted in Vedanta Azure and GCP Cloud)
   j. Security assessment of Email and VPN configuration (Cisco and Fortigate)
   k. Any other
   l. Comprehensive Purple teaming and remediation of findings
   m. Creation of security baseline policies for all asset types above, assist in implementation and perform revalidation
9. Set up an OT security governance desk to perform security risk assessment and vulnerability assessment of connected and isolated systems (present in 9 units and requiring ~23 SPAN ports for traffic capture), assist in remediation and perform revalidation by coordinating with various OEMs (such as Rockwell, Honeywell, Cisco, Schneider, Emerson, Siemens, Hollysys etc.) and corresponding plant SPOCs. Number of SPAN ports mentioned is indicative and will need to be finalised during security risk assessment phase. Following activities will form part of scope:
   a. OT system design and architecture review
   b. System configuration and asset inventory identification
   c. Physical and environment security review
   d. Internet exposure and patching mechanism review

e. Historian and data transfer mechanism review
f. Access management and antivirus setup review
g. Backup and recovery process review
h. Vendor risk review
i. Change management process review
j. Documentation review and OT security policy and procedure upliftment in alignment with IEC 62443 and NIST
k. MBSS creation and implementation assistance in alignment with IEC 62443 and NIST
l. Vulnerability assessment of servers, workstations, PLC, HMI, RTU, DCS, SCADA systems etc.
m. Implementation assistance and revalidation
n. Conduct plant-level workshops, awareness trainings and table-top exercises as required
o. Other administrative/hygiene controls as recommended by selected agency

10. Prepare comprehensive cyber crisis management plan (CCMP) covering all plants and corporate offices. Conduct semi-annual cyber drills involving cross-functional business teams, executive management, Vendor SPOCs etc.
11. Perform internal audit of HZL IT processes and OT processes before commencement of Corporate Management Assurance Audit (MAS) in October.

Critical information regarding Bidding

S/No.	Information	Details
1	Last date for submission of written queries/clarifications	13 February 2025
2	Location of supply	Hindustan Zinc Limited, Yashad Bhawan, Udaipur–313 004, Rajasthan, INDIA.
3	Name of Authority	Chief Information Security Officer
4	Eligible firms	Global Consultancy firms/System Integrators/Professional Services firms having similar demonstrable experience
5	Date of submission of EOI	15 February 2025
6	Contact Person	Information Security Officer, Hindustan Zinc Limited, Yashad Bhawan, Udaipur–313 004, Rajasthan, INDIA.
7	Email	HZL.ISMS@vedanta.co.in
8	Selection process	Stage 1 – Expression of Interest Stage 2 – Techno-commercial proposal submission and evaluation