|  |  |  |
| --- | --- | --- |
| # | **Question** | **Answer** |
|  | 1. There is no Gartner magic quadrant for CTEM but there is a IDC Marketscape for worldwide exposure management, may this be used instead?  2. ⁠There is no certificate for accreditation to IEC 62443. IEC 62443 is not a single certificate or monolithic framework. Rather, it is a modular series of international standards developed to secure Industrial Automation and Control Systems (IACS) — from individual components to entire systems — across their full lifecycle.  The onus will be on Eskom to comply. We will assist in this specific implementation relative to this product, but the set of standards will be applicable to the OT environment across the Eskom estate. Please see some information below:  The IEC 62443 standard is divided into several parts, each focusing on different aspects of cybersecurity for industrial automation and control systems:  The IEC 62443 series is grouped in 4 main categories, each targeting different security aspects of industrial automation. Each category is denoted by the suffixes -1, -2, -3, and -4.   1. General (IEC 62443-1): Provides a complete overview of the IEC 62443 security process and covers terms, concepts, and models that are found throughout the series of standards. It includes foundational documentation that helps in understanding the overall framework. 2. Policies and Procedures (IEC 62443-2): Guides the establishment of an effective cybersecurity program within IACS using policies, procedures, and management practices. It outlines the requirement for the end user or asset owner to develop and implement security management systems. 3. System (IEC 62443-3): Addresses security requirements at the system level to design and implement a secure IACS. It involves risk assessment, system design, and the application of security technologies in IACS environments. 4. Component (IEC 62443-4): Describes the development life cycle requirements, technical functionality and security requirements for industrial network components within the system. From development to deployment of a product, it ensures that every component meets the security standard.   **How to comply with IEC 62443**  IEC 62443 provides precise guidance on maintaining secure development of industrial automation and control systems(IACS). Complying with IEC 62443 involves a systematic approach. To comply with IEC 62443, industrial organizations (eg Eskom) should implement a security management system(SMS) that includes these steps:  Risk Assessment: Conduct a comprehensive risk assessment to identify the company’s risks, determine appropriate security levels and know the critical assets to the ICS.  Developing Security Plan: Develop a security plan that outlines the objectives to secure the ICS (industrial control systems) .  Implementation of Security Controls: Mitigate the identified risks by implementing appropriate security controls.  Verification of Security Controls: Verify that the security controls are implemented correctly and are effective in mitigating the risks.  Regularly Monitoring: Monitor and maintain the security controls to ensure zero risk in future.  Compliance: Regularly assess the Security Management Systems (SMS) to make sure it complies with the standard and is effective in protecting the ICS.  The above is clear that the onus is on the industrial organization to comply, and not the service provider to provide compliance. Our technology stack follows all the appropriate procedures to ensure that on implementation, the system will contribute to the exiting compliance that Eskom must have in terms of IEC 62443.  As there is no specific certification, what will constitute compliance to the IEC 62443 requirement in the tender. | 1.Yes, since Gartner has not yet published a Magic Quadrant for Continuous Threat Exposure Management (CTEM), the IDC MarketScape for Worldwide Exposure Management serves as a valid reference point. IDC’s assessment specifically evaluates vendors with capabilities that align to Gartner’s CTEM framework, covering IT, OT, and hybrid environments.  2. Yes, in the absence of a specific certification, a CTEM platform’s compliance with the IEC 62443 standard must be demonstrated indirectly by evidencing how its capabilities and outputs align with the standard’s requirements.  This is achieved through evident alignment with the relevant IEC 62443 clauses. Refer below the attached **Table 1: CTEM -- IEC 62443 Compliance Mapping Matrix,** for details. |

**Table 1: CTEM -- IEC 62443 Compliance Mapping Matrix**

|  |  |  |  |
| --- | --- | --- | --- |
| **IEC 62443 Clause Requirement** | **Requirement Description** | **CTEM Capability Alignment** | **Example Evidence** |
| IEC 62443-2-1: Policies & Procedures | Define and maintain security policies, roles, and procedures. | Governance dashboards and risk prioritization to inform security policies and workflows. | Policy-aligned exposure reports, governance dashboards, audit logs of risk prioritization. |
| IEC 62443-3-2: Risk Assessment | Perform and maintain risk assessments for IACS. | Continuous validation of exploitable threats, contextualized to business/OT assets. | Continuous risk exposure reports, attack path analysis, documented asset criticality mapping. |
| IEC 62443-3-3: SR 7.6 (Continuous Monitoring) | Continuous monitoring of security events. | Integration with SIEM/SOAR to provide validated exposure intelligence and near real-time threat insights. | Integration logs, alert correlation evidence, incident response playbooks referencing CTEM data. |
| IEC 62443-3-3: SR 1.x – Identification & Authentication | Ensure proper identity and access controls. | Validates exposure of weak credentials and misconfigurations via exploit simulation. | Credential exposure findings, reports on failed/successful login exploit attempts. |
| IEC 62443-3-3: SR 3.x – System Integrity | Protect system integrity against malicious code and unauthorized changes. | Simulates attack scenarios (malware drop, privilege escalation) to validate control effectiveness. | Reports showing blocked vs successful simulated exploits, change detection validation logs. |
| IEC 62443-3-3: SR 5.x – Resource Availability | Ensure system availability and resilience against DoS. | Tests resilience of OT/IT systems to exploit chains that could impact availability. | Exposure validation of DoS attack paths, availability test reports. |
| IEC 62443-4-2: Component Requirements | Component-level security controls for IACS devices. | Validates exposure at PLCs, HMIs, gateways, mapped to IEC 62443 component SRs. | Vulnerability validation reports per component, exploit simulation outcomes. |
| IEC 62443 Security Levels (SL1–SL4) | Assign and validate security levels per system zone/conduit. | Validates control effectiveness to ensure SL target is achieved (e.g., SL2 = resist intentional misuse). | Security level validation matrix, mapped exposure metrics, CTEM test reports vs SL objectives. |
| IEC 62443 Lifecycle Requirements | Continuous improvement of security posture. | Enforces exposure management cycle:   1. Scoping 2. Discovery 3. Prioritization 4. Validation 5. Mobilization. | Continuous improvement logs, remediation workflows, trending exposure metrics over time. |