CLAROTY

- **What is Claroty?**

(ans): Claroty empowers organizations to secure cyber-physical systems across industrial (OT), healthcare (IoMT), and enterprise (IoT) environments: the Extended Internet of Things (XIoT). The company's unified platform integrates with customers' existing infrastructure to provide a full range of controls for visibility, risk and vulnerability management, threat detection, and secure remote access. Backed by the world's largest investment firms and industrial automation vendors, Claroty is deployed by hundreds of organizations at thousands of sites globally.

- **Products of claroty which are used now a days.**

(ans): Products of clarity that are used now a days are as follows:

1. Claroty xDome.
2. Claroty Edge
3. Claroty Secure Remote Access(SRA)
4. Claroty Continuous Threat Detection(CTD).

- What is Claroty xDome?

(ans): Claroty xDome is a highly flexible solution that covers your entire industrial cybersecurity journey. Claroty xDome is a modular, SaaS-powered industrial cybersecurity platform that scales to protect your environment and

- Key Features of Claroty xDome.

(ans): Key Features of the Claroty xDome are as follows:

1. Extends cybersecurity across your in industrial all XIot Devices:

A broad range of XIoT assets underpin your industrial environment: from PLCs, RTUs, and actuators, to smart HVAC and lighting systems. xDome secures them all.

2. Support your all full Cybersecurity to your industry:

Whether you want to automate asset discovery, combat zero-day attacks, or aren't sure where to start, xDome will support and grow with you on your entire journey.

3. It is designed for Scalability, Flexibility and it is easy to use:

As a SaaS solution with a flexible UI built to adapt to all OT, security, and executive needs, xDome deploys and scales effortlessly no matter the user or use case.

4. Integrates seamlessly with your existing tech stack:

xDome's extensive technical ecosystem empowers you to easily extend your existing security and operational infrastructure to your industrial environment.

- Things that can be done by Claroty xDome.

(ans): Things that can be achieved by Claroty xDome are as follows:

1. Asset Discovery with xDome.
2. Asset Management with xDome.
3. Vulnerability and Risk Management with xDome.
4. Network protection with xDome.
5. Threat Detection with xDome.

- Asset Discovery with using Claroty xDome.

(ans): 1. Challenges in Industrial Asset Discovery are as follows:

a. Proprietary Protocols Previal.

Operational technology (OT), building management systems (BMS), and other types of industrial assets use proprietary protocols that are simply incompatible with — and thus invisible to — generalized security tools.

b. Diverse Assets are Default.

Industrial assets can have a decades-long lifespan, so your environment likely has a diverse mix of new and legacy devices that operate and communicate differently.

c. Network Complexity is Norm.

Industrial environments often comprise complex network architectures that include serial or air-gapped sections and are widely distributed across multiple physical sites.

d. One-Size-Fits-All Discovery is a Myth.

Passive monitoring is often touted as a 100% effective, one-size-fits-all method for asset discovery. This is false. A full XIoT asset inventory requires multiple methods.

2. How Claroty xDome solves the challenges of Asset Discovery?

(ans): The following are the ways to challenges of Asset Discovery:

a. Supports 450+ Proprietary Protocols.
b. Delivers 3-D Visibility across industrial XIot.
c. Offers Multiple Methods for Discovery.
d. Harness Expertise Trusted by Industry Leaders.

- Asset Management Using Claroty xDome.

(ans): 1. Challenges in Industrial Asset Management are as follows:

a. Asset Inventory Limitations Persist.

Since industrial assets use proprietary protocols that are incompatible with standard inventory tools, manually maintained, error-prone inventories remain common.

b. Operational Risks are Emerging Rapidly.

Manual asset management processes are no match for the pace at which vulnerabilities, end-of-life indicators, outdated firmware, and other operational risks emerge.

c. Compliance Requirements are Stringent.

Complying with asset SLAs and audits requires tracking and reporting on granular asset insights that standard tools or manual processes simply cannot provide.

2. How Claroty xDome solves the challenges of Asset Management?

(ans): The following are the ways to challenges of Asset Management:

a. Automates and Enriches your Asset Inventory.
b. Continuous Monitoring for Operation Risks.
c. Optimizes Workflows via Reporting and Integrations

- Vulnerability and Risk Management Using Claroty xDome.

(ans): 1. Challenges in Vulnerability and Risk Management are as follows:

a. Asset Visibility is Often Minimal.

Industrial assets use protocols that are largely invisible to standard security tools. If you can’t identify an asset, you definitely can’t manage its vulnerabilities and risks.

b. Context Gaps Hinder Prioritization.

Finding a vulnerability isn’t enough. You also need to assess the affected asset’s context and potential impact on your operations to prioritize and remediate the risk.

c. Vulnerability Scanners are Unsafe.

Industrial environments and the assets that underpin them are uniquely fragile and cannot tolerate the traffic generated by standard vulnerability scanners.

d. Patching is Rarely Permitted.

Most industrial environments have no tolerance for downtime, so maintenance windows (and, as a result, patching) occur rarely, no matter the vulnerability or risk.

2. How Claroty xDome solves the challenges of Vulnerability and Risk Management?

(ans): The following are the ways to challenges of Vulnerability and Risk Management:

a. Discovers, Enriches and Correlates Your Assets.
b. Optimizes Prioritization with custom Risk Scoring.
c. Safely Eliminates Risk Blindspots with Integration.
d. Drives Actions to Enhance risk posture.

- Network protection Using Claroty xDome.

(ans): 1. Challenges in Network protection are as follows:

a. Segmentation Policies are Error-Prone.

Effectively segmenting industrial networks can be a tedious, error-prone process that entails defining and constantly tuning policies to your unique environment.

b. Compliance is Inconsistently Enforced.

Monitoring and ensuring compliance with regulatory and organizational measures requires granular, properly tuned policies that many organizations lack.

c. Unsecured Remote Access is Widespread.

All industrial environments rely on remote access to enable both internal and third-party personnel to maintain assets, but common practices are risky and inefficient.

2. How Claroty xDome solves the challenges of Network protection?

(ans): The following are the ways to challenges of Network protection:

a. Jumpstarts and Optimizes Network Segmenttation.
b. Automates Policy Compliance Monitoring.
c. Secures, Controls, and Streamline Remote Access.

- Threat Detection Using Claroty xDome.

(ans):1. Challenges in Threat Detection are as follows:

a. Traditional Monitoring Tools are Incompatible.

The proprietary protocols in industrial environments are not compatible with traditional threat detection tools, rendering them ineffective and potentially disruptive.

b. Industrial Environments are complex.

The intricacy of multisite industrial environments and their critical assets can make it difficult to identify potentially malicious deviations from accepted baselines.

c. Targeted Attacks are on Rise.

Industrial environments are increasingly targeted by malicious actors due to their growing XIoT attack surface, inherent insecurity, and downtime intolerance.

d. Expertise and SOC Functional Gaps.

Many security operations center (SOC) teams are trained to detect and respond to IT-centric incidents but lack the domain-specific knowledge and tools needed to defend industrial environments.

2. How Claroty xDome solves the challenges of Threat Detection?

(ans): The following are the ways to challenges of Threat Detection:

a. Purpose-Built Monitoring for Industrial Environments.
b. Streamlines Threat Alerting and Minimizes False Positives.
c. Easily Identifying and Remediating Attack Vectors.
d. Seamlessly Extends Existing SOC Capabilities.

- What is Claroty Edge?

(ans): Claroty Edge is a first-of-its-kind collection method that provides truly unmatched visibility into industrial environments in minutes with no additional hardware, no configuration, and no risk of disruption.

Designed for ease and flexibility, Claroty Edge combines effortlessly with our other collection methods to reflect two core tenets of our industrial cybersecurity portfolio:

1. Claroty recognizes there is no one-size-fits-all path to asset discovery because each customer, environment, and cybersecurity journey is unique.
2. We also recognize that achieving truly complete, real-time visibility into any industrial environment almost always requires leveraging not only Claroty Edge or any other singular collection method but a combination of multiple methods. This limitation isn't a weakness of our technology it’s a vendor-agnostic reality of collection itself.

- Key Features of Claroty Edge.

(ans): The key Features of Claroty Edge are as follows:

a. Builds the foundation for cybersecurity maturity:

The in-depth XIoT asset, risk, and vulnerability details Edge provides is foundational to all other phases of your industrial cybersecurity maturity journey.

b. Supports multi-disciplinary use cases:

The speed and ease with which Edge operates makes it suitable to support a range of multidisciplinary use cases: from incident response, to audits, to M&A due-diligence.

c. Requires zero network changes or hardware:

Since Edge leverages your existing infrastructure and is safe and compatible with all environments, you won't need to purchase hardware or make changes to utilize it.

d. Offers unmatched time-to-value:

Five-to-ten minutes is the average amount of time it takes to deploy, run, and gain full visibility into all assets, risks, and vulnerabilities in your environment with Edge.

- Things that can be done by Claroty Edge.

(ans): Things that can be achieved by Claroty Edge are as follows:

1. Asset Discovery with Claroty Edge.
2. Vulnerability and Risk Management with Claroty Edge.
3. Audit, Compliance and Due Diligence with Claroty Edge.
4. Incident Response with Claroty Edge.

- What are the collection methods of Claroty?

(ans) The collection methods of Claroty are as follows:

1. Passive monitoring
2. Safe Queries
3. Project File Analysis
4. Ecosystem Enrichment

- What is Passive Monitoring in Claroty?

(ans) Claroty's approach to Passive Monitoring offers continuous visibility into industrial environments by fusing our leading protocol coverage and DPI (Deep Packet Inspection) technology with unmatched flexibility that enables customers to easily combine this collection method with any of our four others to suit their needs.

This approach also embodies two tenets of our industrial cybersecurity portfolio:

1. We recognize there is no one-size-fits-all collection method or approach to XIoT asset discovery because each customer, OT environment, and industrial cybersecurity journey is unique.
2. we also recognize that to achieve a truly comprehensive asset inventory, Passive Monitoring (or any singular collection method) alone won’t cut it. Most customers seeking 100% visibility must combine multiple methods to get there.

- Key Benefits of Passive Monitoring.

(ans): Key Benefits of Passive Monitoring are as follows:

1. Non-Disruptive:

Passive Monitoring creates no additional traffic and does not interact directly with assets. As a result, it has no impact on the OT environment and thus poses no risk to operational availability, integrity, or safety.

2. Effective:

A key reason why Passive Monitoring has long been the industry’s status quo for asset discovery is that it can typically identify and reveal rich details on most types of XIoT assets within most OT environments.

3. Continuous:

Passive Monitoring analyzes traffic continuously, enabling it to not only pinpoint any changes in the OT environment — but also automatically update the asset inventory to reflect those changes in real-time.

4. Multipurpose:

Beyond discovering assets, Passive Monitoring also delivers visibility into communication baselines, operational behaviours, potential threats, and other insights integral across the industrial cybersecurity journey.

- Working of Passive Monitoring .

(ans): Passive Monitoring works by reconfiguring a switch in the OT network with a SPAN, mirror, or monitor port to copy the packets of traffic sent between the network's assets. These copied data points are then sent to an on-premise or cloud-based server for analysis via deep packet inspection (DPI), which identifies the respective assets and their vendor, model, operating system, and other details.

The depth and accuracy of these details are critical to the effectiveness and efficiency of a range of subsequent use cases such as asset management, vulnerability and risk management, Network protection, Threat protection and more.

- Is Passive Monitoring unique to Claroty?

(ans): Passive Monitoring is the status-quo collection method for asset discovery in industrial environments. But while the method itself is widely available in the market, Claroty's approach is differentiated.

Unlike other vendors' offerings, the Passive Monitoring built-in to Claroty CTD and xDome can be easily combined with our other collection methods to suit each customer's needs. Since our solutions also support an unmatched 450+ protocols, they are uniquely compatible with — and able to discover — even the most obscure types of OT, IoT, and other XIot Assests.

- Limitations of Passive Monitoring.

(ans): Limitations of Passive Monitoring are as follows:

Since Passive Monitoring works by inspecting traffic, it is not suitable for discovering assets that seldom communicate (and, thus, seldom generate traffic). The redundant assets typically found in electric grids and that only communicate in failover situations are among many common examples of this. But even among assets that do generate traffic frequently, some are still problematic for Passive Monitoring due to their specific protocols.

Example:

Modbus, a protocol widely used by BMS assets, typically reveals very little about an asset in its communications. So while Passive Monitoring might be able to identify that a Modbus asset is, for instance, an elevator, it may not be able to pinpoint its vendor, firmware, or other details that are key to protecting that elevator and the critical function it serves.

- Can Passive Monitoring can deliver 100% visibility or not?

(ans): While Claroty's approach to Passive Monitoring makes it highly effective, no singular collection method (whether from Claroty or elsewhere) is a silver bullet. Passive Monitoring in particular simply cannot discover certain types of assets and details due to how they communicate and other limitations that exist to varying degrees in nearly all industrial environments. Unfortunately, this reality can be easy to overlook amid the abundance of misinformation and misleading claims from other vendors — most of which offer only Passive Monitoring as their sole collection mention.

Recognizing how crucial it is for our customers to have 100% visibility into the assets that underpin their operations, Claroty has long been committed to delivering it. This is why we're proud to be the only vendor to offer five distinct collection methods. While using Passive Monitoring alone will nearly always be insufficient, combining it with our Safe Queries, Claroty Edge, and/or other methods has been consistently proven to empower our customers with the truly full visibility they need (and can't get anywhere else).

- What are the reasons which makes Passive Monitoring safe for OT networks?

(ans): Passive Monitoring has long been proven safe for even the most fragile, critical, and complex OT networks because it does not touch, alter, or otherwise impact any assets or operations.

Most concerns around potential risks to OT availability, integrity, and/or safety stem from the use of technologies or mechanisms that are not purpose-built for OT networks and/or that otherwise generate traffic that OT systems simply cannot tolerate. Since Passive Monitoring generates no traffic whatsoever and, at least in the context of Claroty's portfolio, is only offered within solutions that are truly purpose-built for OT it does not pose any such risks.

- What is Safe Queries in Claroty?

(ans): As Claroty's version of what the industry refers to as active scanning, Safe Queries fuse our proven-safe technology with unmatched flexibility that lets customers easily combine this collection method with any of our four others based on their XIot asset discovery needs.

- Key Benefits of Safe Queries.

(ans): Key Benefits of Safe Queries are as follows:

1. Safe:

Recognizing the risks posed by standard active scans, we've built, extensively tested, and proven our Safe Queries to be truly safe for all XIoT assets. This caliber of safety has even been validated by manufacturers of the industrial assets themselves.

2. Precise:

The precision and depth of visibility typically provided by Safe Queries is largely unmatched even when this method is utilized to discover assets and/or asset-level details that other collection methods are unable to adequately pinpoint.

3. Efficient:

Safe Queries offer an exceptionally speedy time-to-value (TTV). This collection method is consistently able to return robust, granular visibility results quickly, easily, and without requiring extensive sensors or other hardware installations.

- Working of the Safe Queries.

(ans): Claroty's Safe Queries work by sending targeted, non-disruptive communications to certain segments of the industrial environment and reporting back on which assets are present and what their key details such as firmware versions, patch levels, and more are.

Safe Queries are often used to supplement other collection methods when deeper details about a specific asset or segment are needed. A common example is when Passive Monitoring discovers an asset's type and protocol but little else due to various limitations. Using those basic details provided by passive monitoring, Safe Queries can then exchange targeted communications with that asset to quickly and easily gather its remaining details.

- Can Safe Queries are truly safe for OT Network?

(ans): Yes. While traditional approaches to active scanning have rightfully earned a reputation of being disruptive and even dangerous to OT environments we designed Claroty's Safe Queries in a manner that virtually eliminates these risks.

Specifically, the biggest concerns around active scans are those that generate more and/or different traffic than what an asset can handle. Safe Queries do just the opposite: they mimic the exact amount and type of traffic an asset is already accustomed to receiving from the other assets with which it communicates. This traffic is also sent in the asset's native protocol, further ensuring it does not encumber the network and cannot be distinguished as related to anything but the OT environment's standard operations.

- Limitations of Safe Queries.

(ans): The Limitations of Safe Queries are as follows:

Since this collection method works by exchanging communications with assets, it is ineffective at discovering assets that lack properly functioning communication mechanisms. Although it is relatively rare, this can happen when an original equipment manufacturer (OEM) or operator inadvertently or otherwise disables an asset's ability to respond to queries.

This limitation does NOT prevent our customers from gaining 100% visibility. While neither Safe Queries nor any collection method is a silver bullet by itself the right combination of methods absolutely can be. This is why we make it easy for customers to combine Safe Queries with our Passive Monitoring, Claroty Edge, Project File Analysis, and Ecos methods to suit their needs.

- Can Safe Queries support continuous monitoring feature?

(ans): No. Unlike Passive Monitoring, Safe Queries do not continuously inspect the traffic sent between assets in the industrial environment instead, they target and exchange communications with specific assets when needed. The deep visibility provided by this method reflects the point in time at which such communications are exchanged.

For customers seeking continuous monitoring (such as to support threat detection, change management, and related use cases), we enable and encourage them to combine our Safe Queries, Claroty Edge, and/or other methods with our Passive Monitoring. This type of combination ensures full, real-time visibility and cybersecurity coverage without compromise.

- What is Project File Analysis in clarity?

(ans): Claroty's Project File Analysis harnesses a unique file-parsing mechanism to provide deep visibility into XIoT assets even those in truly air-gapped industrial environments.

- Key Benefits of Project File Analysis.

(ans): Key Benefits of Project File Analysis are as follows:

1. Non-Intrusive:

Project File Analysis is uniquely non-intrusive because it relies on parsing files that are typically stored in offline repositories. As such, this collection method has no impact whatsoever on operational availability, process integrity, or safety.

2. Powerful:

This collection method can deliver efficient, effective visibility into assets and asset details even under challenging circumstances where most other collection methods would fall short — such as in fully air-gapped environments, for example.

3. Fast:

Since Project File Analysis does not require lengthy installations or direct connectivity to the industrial environment, it can deliver deep visibility rapidly and even help expedite implementations of other Claroty offerings by blueprinting their deployments.

- Working of Project File Analysis.

(ans): Working of Project File Analysis are as follows:

Claroty's Project File Analysis works by ingesting and parsing the configuration files that are routinely backed-up on workstations and other support and management components of industrial environments. These files typically include details used by or related to industrial assets like PLCs and RTUs, as well as other assets with which those PLCs and RTUs communicate, making them rich information sources on virtually all assets in the environment.

Since this collection method does not require direct connectivity to the industrial environment itself, it is even suitable for those that are air-gapped or otherwise largely inaccessible.

- Limitations of Project File Analysis.

(ans): Limitations of Project File Analysis are as follows:

Since the deep visibility provided by Project File Analysis is extracted from back-ups of configuration files its timeliness depends on how often these files are backed-up.

While backups happen extremely frequently in many industrial environments, they seldom occur in others. For those in which asset changes are a common occurrence yet backups are not, relying solely on Project File Analysis can result in an outdated asset inventory. As a result, we encourage (and make it easy for) customers to combine Project File Analysis with one or more of our other collection methods to keep their asset inventory up-to-date.

- Which are the other collection methods best complement Project File Analysis?

(ans): Just as every customer is unique, every combination of our five collection methods has its own unique benefits and rationales. That being said, most of our customers who choose to use our Project File Analysis also use our Passive Monitoring.

A common scenario is for customers to first deploy Project File Analysis to rapidly discover their assets. Using their newly obtained asset inventory as a blueprint, customers can then more easily, effectively, and efficiently deploy Passive Monitoring to extend or support threat detection, segmentation, and other Industrial Cybersecurity controls across their environment.

- What is Ecosystem Enrichment in Claroty?

(ans): Claroty's Ecosystem Enrichment collection method enhances and unifies visibility of XIoT assets and related insights by empowering customers to capitalize on the rich information harbored within their existing CMDB(Configuration Management Database), disaster recovery, EDR(Endpoint Detection and Response), and other cybersecurity and operational technologies.

- Key Benefits of the Ecosystem Enrichment.

(ans): Key Benefits of the Ecosystem Enrichment are as follows:

1. Unified XIoT Visibility:

From plant managers, to network administrators, to security operations center teams, to procurement specialists, and more numerous business functions require an up-to-date, enterprise-wide asset inventory to execute their essential workflows, yet few manage to truly attain it. Ecosystem Enrichment helps banish these siloes by correlating and centralizing the rich information harbored within these functions' existing tools to deliver a unified, single source of truth for all IT-XIoT asset details.

2. Stronger XIoT Protection:

Beyond enhancing XIoT visibility, many of the integrations that underpin Ecosystem Enrichment also extend added protective controls across the XIoT. Claroty's extensive joint portfolios with endpoint protection leader and version CrowdStrike control innovator Auvesy, for example, each offer plug-and-play integrations that not only enrich and reconcile XIoT asset inventories but also boost protection against IT-XIoT threats while optimizing disaster recovery capabilities, among others.

3. Unmatched ROI, TCO, and TTV:

While the enhanced XIoT visibility and protection provided by Ecosystem Enrichment are notable in themselves, another key differentiator of this collection method is its ability to deliver added value across the business. Since this method relies on (and derives greater value from) customers' existing investments, it thereby increases the value of those investments without burdening users with complex learning curves. The result is better protection and a more efficient workforce at a reduced cost.

ROI- Return of Investment

TOC- Technology Optimization Center

TTV- Time to Value.

- Which are top integrations for Ecosystem Enrichment in Claroty?

(ans): The top integrations for Ecosystem Enrichment are as follows:

1. CrowdStrike
2. ServiceNow
3. Rockwell Automation
4. Auvesy

- What is Claroty Secure Remote Access(SRA)?

(ans): Claroty SRA delivers frictionless, reliable, and highly secure remote access to industrial environments for internal and third-party users.

- Key Benefits of Secure Remote Access.

(ans): Key Benefits of Secure Remote Access are as follows:

1. Streamlines Access for Internal and Third-Parites:

SRA removes the complexity and administrative barriers to effective, efficient remote access to industrial environments for both internal and third-party users.

2. Extends Zero Trust-based Access Controls:

Remote access is the most commonly exploited attack vector for industrial environments. SRA eliminates this with a secure architecture and granular access controls.

3. Offers Full Auditing Response Capabilities:

All SRA user sessions enable live, over-the-shoulder monitoring, live disconnects if needed, and full-length recordings to support audit requests and investigations.

4. Delivers an Ideal UX that Reduces MTTR:’

SRA’s purpose-built user experience makes connecting, troubleshooting, and repairing assets fast and easy, no matter where assets or users are located.

MTTR- Mean Time To Respond

- Things that can be done by Claroty SRA.

(ans): Things that can be done by Claroty SRA are as follows:

1. Remote Maintenance using SRA.
2. Remote Access Administration using SRA.
3. Role-Based Access Control using SRA.
4. Comprehensive Monitoring using SRA.
5. Remote Incident Management using SRA.

- What is the Continuous Threat Detection in Claroty?

(ans): Claroty CTD is a robust solution that delivers comprehensive cybersecurity controls for industrial environments.

- Key Features of the Continuous Threat Detection.

(ans): The key Features of the Continuous Threat Detection are as follows:

1. Provides purpose-built industrial cybersecurity:

CTD isn't another generic solution. It was purpose-built by experts intimately familiar with the unique security and operational needs of industrial environments.

2. Suitable for all goals and maturity levels:

No matter whether you're new to industrial cybersecurity or seeking to optimize an existing program, CTD will meet you wherever you are on your maturity journey.

3. Supports on-premise deployment preferences:

Recognizing that not all organizations are ready or able to embrace SaaS solutions, CTD supports on-premises deployments without compromising on ease or flexibility.

4. Integrates Seamlessly with Claroty SRA:

CTD's native integration with Claroty Secure Remote Access (SRA) enables response and remediation for incidents related to remote user activity.

- Things that can be done by Claroty Continuous Threat Detection.

(ans): Things that can be done by Claroty Continuous Threat Detection are as follows:

1. Asset Discovery using CTD.
2. Network protection using CTD.
3. Vulnerability and risk management using CTD.
4. Threat Detection using CTD.

- Price of Claroty.

(ans): Prices of Claroty are as follows:

PRICE: $ 300000 – Rs.2,47,50,000

Prices of Claroty Edge are as follows:

PRICE: $ 27900- Rs.23,92,500

Prices of Claroty SRA are as follows:

PRICE: **Extra small-size SRA: $3000- Rs.2,47,500**

small-size SRA: $6000- Rs.4,95,000

mid-size: $9000- Rs.7,42,500

Large-size:$13500- Rs.11,13,750

Prices of Claroty CTD are as follows:

PRICE: **Extra small CTD: $ 5900- Rs. 4,86,750**

Small CTD: $19500- Rs. 16,08,750

Mid-size CTD: $29250- Rs. 24,13,125

Large-size CTD: $43875- Rs.36,19,688

Very large-size CTD: $65000- Rs.53,62,500