ApexaIQ Internship Session

1. What does ApexaiQ do? What industry problem does it solve?

ApexaiQ is a platform that gives companies a clear picture of all their IT assets – devices, users, and software – without needing to install agents on every system. It collects data from the tools a company already uses, cleans and enriches that data, and then gives a risk score so teams know which issues to fix first. In short, it helps organizations reduce cyber risk, stay compliant, and keep their IT environment healthy and secure.

ApexaiQ helps companies see all their IT assets, find risks fast, and fix what matters most – all without installing agents

2. Industry problem ApexaiQ Solves

- Visibility gap : Many organizations lack a complete, up-to-date inventory of devices , software and accounts Unknown assets = unknown risk.
- Fragmented telemetry: Security teams get disparate feeds (vulnerabilities, EDR, network scanners, cloud, CMDBs) that aren't correlated.
- Prioritization overload: Too many vulnerabilities/alerts without context (business criticality, exploitability) — teams can't prioritize what to fix first
- Compliance & obsolescence management: Hard to track EoL/EoS and compliance across large fleets.

3. What is IT asset management and why companies need asset management software

ITAM software helps organizations see, secure, and optimize every IT asset — saving money and reducing risk

Why companies need ITAM software

- Visibility: Get a complete inventory of all assets in one place.
- Security: Spot outdated or vulnerable devices and software before attackers exploit them.
- Cost Control: Avoid paying for unused licenses or unnecessary hardware.
- Lifecycle Planning: know when to upgrade or replace assets before they reach

3. 3-5 competitors of Apexaiq and how they are different from Apexa. Case studies.

Tenable (Nessus / tenable.io)-Vulnerability-first

Its mainly focus on vulnerability scanning and exposure management and difference is that strong scanner plus exposure analytics and less emphasis on full ITAM lifecycle or multi-source enrichment and business – critical prioritization out-of-the box

Case Study: financial firm used tenable to scan /sweep workflows but required extra tooling to map vulnerabilities to business critical assets

Qualys -Cloud-based vulnerability and asset inventory

its mainly focus on continuous scanning and assets inventory and cloud posture and difference is that Qualys is strong at large scale discovery and compliance modules;may need additional correlation and prioritized remediation workflows that ApexaiQ provides via rules enrichments

so its case study is that a retail chain standardized on Qualys for PCI compliance scanning but integrated another CMDB to get business context – shows Qualys strength in scanning + compliance

3. CrowdStrike — Endpoint protection + EDR

Crowdstrike is focus on the endpoint detection and response ,threat hunting ,prevention(agent-based). And its difference is that agent based EDR with strong telemetry and response-different architecture from ApexaiQ (agentless). Apexaiq focuses on integrating many sources and asset hygiene/ITAM use-cases

4 Service Now ITSm/ITOM/ITAM-IT operation and governance

Enterprise ITSM/CMDB and its lifecycle and its difference is that service now is a board it operation platform (ticketing ,CMDB workflows) ApexaiQ is specialized in security-focused asset discovery, vulnerability enrichment and prioritized remediation workflows; easier to deploy for security teams than a full ServiceNow implementation.

4. Why is ApexaiQ an agentless platform?

ApexaiQ is agentless so companies get faster setup, wider assets coverage ,and zero performance impact and ApexaiQ is a agentless so companies get faster setup, wider asset coverage ,and zero performance impact and No Installation Needed so ApexaiQ does not require installing agents on every devices and faster Deployments so its Easy to set since its connect directly with existing tools and its covers all asset types such as the printers ,IOT and networks gear

Finding And Research on Cybersecurity

Organization face faster , more sophisticated attacks,bigger supply chain risk, and a growing gap between the number of vulnerabilities and the ability to fix them Effective defense centers on visibility + Prioritization + automation exactly where ApexaiQ adds value

- Current threat landscape :

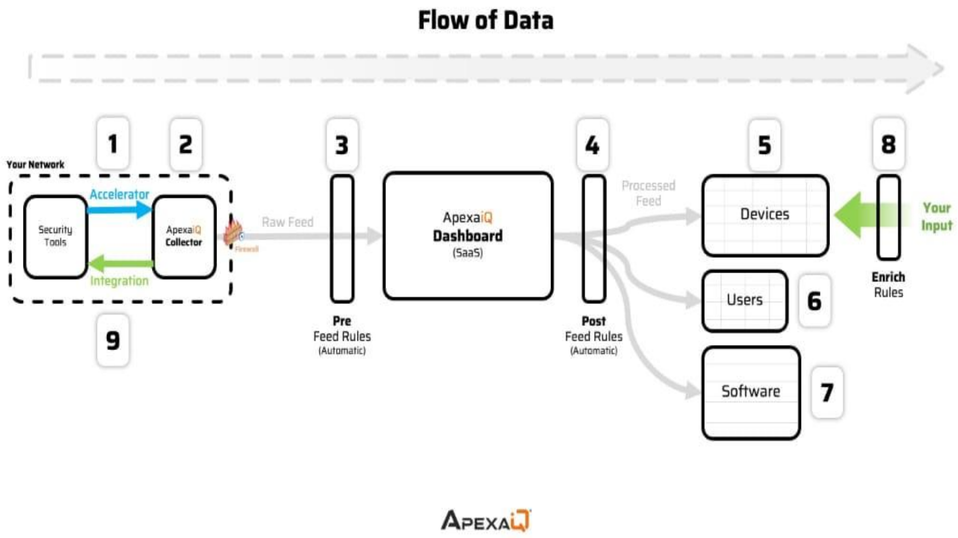
Ransomware and hyrid attacks are still top – tier risks and they now target critical infrastructure

Suppy-chain risk is a top CISo worry .Organization can be compromised through suppliers ,managed services or embedded third party components A 2025 supply chain trends study shows strong ,persistent concern about visibility and remediation across suppliers

- Vulnerability And CVE reality

The volume of disclosed vulnerabities and cves has increased sharply NVD processing and backlog issues mean not every CVEs is evaluated quickly,making automation and prioritized remediation essential and its practical implications is that don’t try to patch everything at once – prioritizd by exploitability business criticality and exposure

- Attack surface and asset visibility
  Attack surface = all externally and internally reachable assets .without a single source of truth ,teams connot prioritize risk properly



1 Security Tools (Your Network)

- These are existing tools in your IT environment (firewalls, EDR, vulnerability scanners, SIEMs, cloud APIs, etc.).
- They already generate data about devices, users, and software.

2 Accelerator + Collector (Integration Layer)

- Accelerator: Connects and integrates with your security tools.
- ApexaiQ Collector: Collects the raw feed (logs, alerts, asset data) without installing agents.

3 Pre-Feed Rules (Automatic)

- Before sending data to the dashboard, automatic pre-processing rules clean, filter, and normalize the raw feed.
- Removes noise or duplicate entries.

4 ApexaiQ Dashboard (SaaS)

- The central SaaS platform where the processed data is displayed.
- Security teams see assets, risks, and compliance status in one place.

5 Devices

- Processed data gets mapped to devices (laptops, servers, IoT, etc.).

6 Users

- User-related information (logins, accounts, access patterns) is tracked.

Software

- Information about installed applications, licenses, and usage is categorized.

7 Enrich Rules (Your Input)

Security teams can add business context:

- Tagging critical assets
- Defining compliance policies
- Adding prioritization rules.

- This enriches the processed feed for better decision-making.

8 Integration (Feedback Loop)

Enriched and categorized data can be fed back into your existing security tools for automation and remediation.

ApexaiQ works like a bridge between your existing security tools and actionable insights.

- It collects raw data,
- cleans and processes it,
- organizes it by devices, users, and software,