|  |  |
| --- | --- |
| Unlock Asset Clarity: Secure, Compliant ... | **ApexaiQ Internship Documentation** Prepared by: Swami Ganesh Deshpande Intern - ApexaiQ |

|  |
| --- |
| **1. What does ApexaiQ do? What industry problem does it solve?**  ApexaiQ is a cybersecurity and IT asset intelligence platform. It helps organizations manage, monitor, and secure their digital assets without using traditional software agents. The platform focuses on Cyber Asset Attack Surface Management (CAASM), allowing businesses to gain real-time visibility into all devices, applications, and network assets. The main problem it solves is the lack of visibility in IT environments, which often leads to vulnerabilities, compliance risks, and cyberattacks. |

|  |
| --- |
| **2. What is IT Asset Management and why do companies need it?**  IT Asset Management (ITAM) is the practice of tracking, managing, and optimizing all the hardware, software, and network assets of an organization. Companies need ITAM to: - Reduce unnecessary costs. - Stay compliant with regulations. - Improve cybersecurity by knowing which devices and software are in use. - Manage asset lifecycle (purchase to retirement). - Identify vulnerabilities and keep systems updated. |

|  |
| --- |
| **3. Competitors of ApexaiQ and Case Studies**  Some competitors of ApexaiQ include: 1. Axonius – Provides a similar agentless asset management platform but can be complex for smaller organisations. 2. JupiterOne – Focuses on cyber asset visibility but is more developer-centric compared to ApexaiQ. 3. Qualys – Strong vulnerability and compliance tools but often relies on agents for full coverage. 4. ServiceNow – Best known for ITSM and ITAM workflows; broader but not purely focused on CAASM.  Case Study Example: A mid-sized financial company struggled with asset visibility and compliance audits. After adopting ApexaiQ, they mapped all assets within days, identified outdated systems, and reduced audit preparation time by 40% through automated reporting and prioritized remediation. |

|  |
| --- |
| **4. Why is ApexaiQ an agentless platform?**  ApexaiQ is agentless because it does not require installing additional software on every device. Instead, it integrates directly with existing IT systems, cloud services, and security tools to gather data. This makes deployment faster, reduces maintenance overhead, and avoids performance issues caused by heavy agents. |

|  |
| --- |
| **5. Research and Findings on Cybersecurity**  Cybersecurity means protecting systems, networks and data from digital attacks. Short, practical findings for an intern: - Human error is a major cause of breaches. - Knowing all assets reduces risks. - Regular patching and compliance checks are essential. - Zero Trust and CAASM approaches are increasingly used to limit attack surface. |

|  |
| --- |
| **6. Key Concepts (short definitions)**  ApexaiQ Score – A rating showing the health and security posture of IT assets.  Vulnerabilities – Weaknesses that attackers can exploit.  Obsolescence – When software or hardware becomes outdated.  Compliance – Meeting standards like ISO 27001, HIPAA, etc.  Maintenance – Updates and fixes to keep systems running safely.  End of Life/Support – When vendors stop supporting products.  Asset Hygiene – Keeping assets updated and managed.  Crown Jewel – Most critical business assets (e.g., customer data).  Inventory – A full list of company assets.  NVD – National Vulnerability Database, list of known vulnerabilities.  Patch Management – Applying updates to fix security issues.  Data Breaches – Unauthorized access to data.  MSP – Managed Service Provider, an external IT service company.  Device Types – Servers, laptops, IoT devices, printers, cloud instances, etc. True SaaS – Fully cloud-based software with no on-prem installs.  Inbound/Outbound Integration – Connecting ApexaiQ to other tools for data flow.  Compliance Standards – Examples: CISA guidance, ISO 27001, HIPAA (healthcare).  Perimeter – Network boundary; increasingly blurred with cloud.  ROI & KPI – Measuring value and performance of IT/security efforts.  Auto-remediation – Automatic fixes applied by tools.  Network Protocols – Rules for data transfer (HTTP, TCP/IP).  Due Diligence – Careful checking before a purchase or integration.  SOAR – Tools that orchestrate security tasks automatically.  Role of ITAM in Zero Trust – ITAM provides the asset visibility that Zero Trust needs.  CAASM – Cyber Asset Attack Surface Management: continuous asset visibility and risk reduction. |

