vicarius

Top 5 Questions Clients Answer with TOPIA

vicarius.io   **info@vicarius.io**
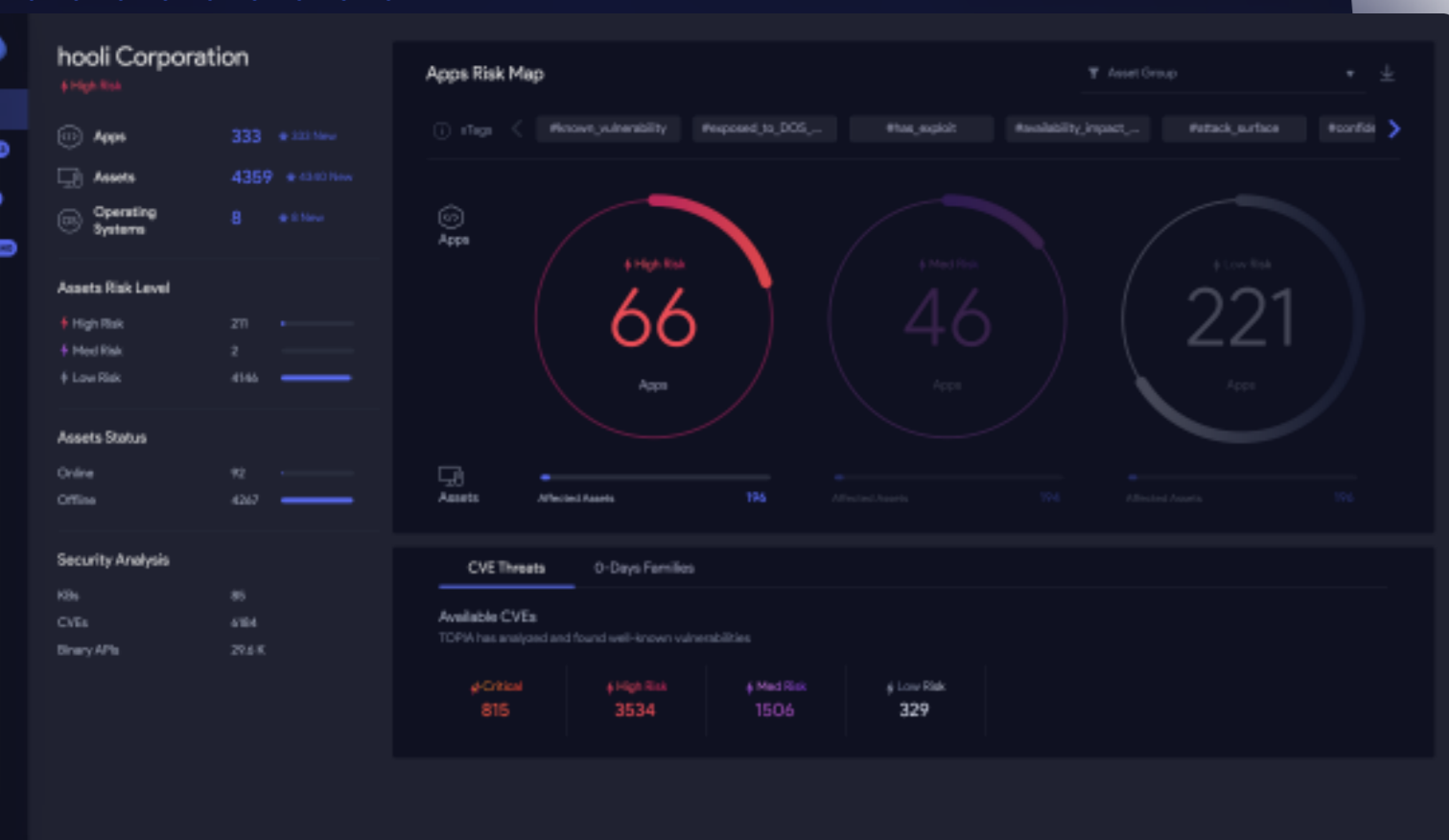
"Do we want to consolidate tools?"

Its common to find three to five tools in a vulnerability management program depending on the size of an organization. This creates complexity in data integrity, process efficiency, and resource utilization. Vicarius takes the core of vulnerability management programs and tightly integrates them. Asset inventory, analysis, prioritization, remediation, and reporting are bundled together to limit the amount of tools required to achieve risk reduction.

"How do we solve work from home use cases affecting risk management?"

As more people work from home and infrastructure becomes decentralized, vulnerability management requires increased flexibility. Vicarius built a Cloud First and Cloud Ready platform that can be flexible for on-premise requirements as well as remote workers and cloud assets. The solution is 100% SaaS with on-premise features to augment use cases like patch distribution.

"How can we make CVSS more accurate to prioritize remediation?"

Many organizations are using subjective business risk scores as their primary. CVSS is both a technical and environmental method for measuring risk. The challenge most unappreciated with CVSS calculations are the temporal and environmental attributes that need to be adjusted to achieve an accurate score. The raw score is not customized on the client environment. Machine data can complete CVSS risk scoring to make the overall program more accurate at the highest risk vulnerabilities. Vicarius automates this process and allows the client to adjust with business risk as they find appropriate.

"How can we prioritize resources better?"

Increasingly the amount of discovered vulnerabilities outweighs the amount of resources available to remediation quickly. The correlation of machine data can prompt better decision-making processes which will focus on the highest risk vulnerabilities to the environment. Business risk scoring alone does not take into account how attackers view the entry and lateral movement in an attack. Machine data correlated with vulnerability information can align resources against the highest risk issues. This data must come from endpoints. Vicarius automates this entire process from data collection to correlation to automated remediation opportunities.

"Do we want to automate remediation activities?"

Traditionally multiple tools make it impossible to build automation through middleware because they are various sources of truth, very little context, and mostly subjective processes. Vicarius removes the subjective risk, automates the machine data collection and correlation for more accurate prioritization. This all enables Vicarius to offer an automation engine to remediate vulnerabilities.