Vuln **Discovery**

Full asset visibility in a single pane of glass

You can't fix what you can't find. TOPIA enables 360-degree asset visibility, illuminating a cloud-based catalog of active servers, workstations, installed applications, and operating systems, putting you in complete control of all asset activity in real-time, for both on-premise and cloud environments.

- ✓ Software and OS Inventory
- ✓ Asset Inventory
- ✓ CVE Visibility
- ✓ Network Scanning

- ✓ Inventory Threat Analysis
- ✓ Vulnerability Management
- ✓ Software Composition Analysis
- ✓ Vulnerability Auto Tracking

Vuln **Prioritization**

Real-time contextualized prioritization

Not all vulnerabilities are created equally. Focus on risks that have real potential for exploitation instead of wasting resources solving problems that don't exist. TOPIA prioritizes software vulnerabilities using industry-standard base metrics alongside an AI-based contextual usage risk-scoring engine, unique to your environment and priorities.

- ✓ Contextual Risk Factoring
- ✓ App and OS Risk Analysis
- ✓ Usage-based Threat Tracking
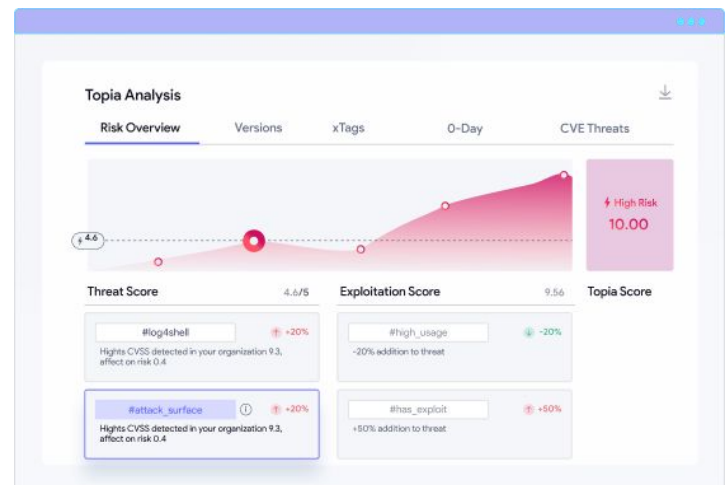
- ✓ xTags™ - Risk Mapping
- ✓ Customized Factor Weighting
- ✓ CVE-intel Data Gathering
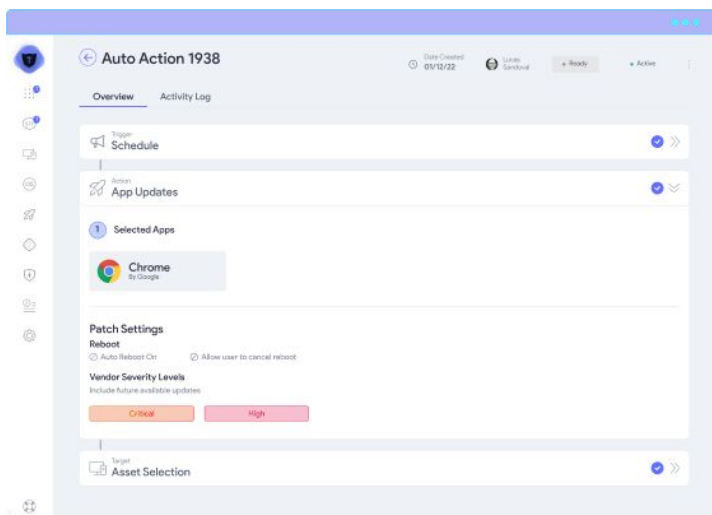
Vuln **Remediation**

Effortlessly find and eliminate threats

Don't just find your flaws. Fix them. TOPIA allows you to quickly test and install patches across your organization's asset inventory with strategic scheduling to minimize business impact and downtime. Integrated patch deployment tools cover Microsoft, Linux, Mac and 3rd party applications from a single dashboard to efficiently target all risks.

- ✓ Patch Management
- ✓ Patchless Protection™
- ✓ Scripting
- ✓ Asset-Group Rollouts
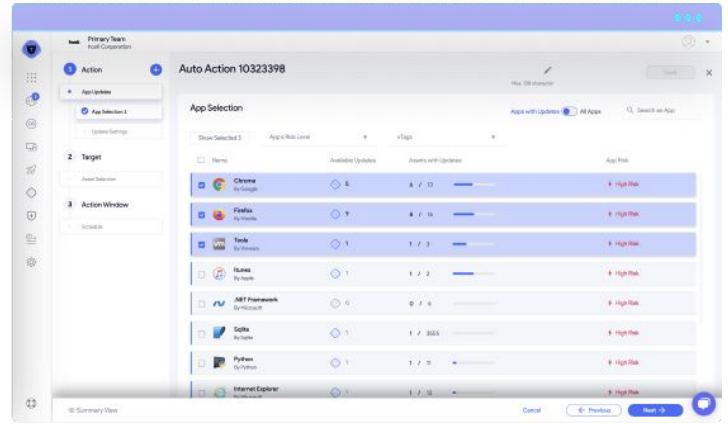
- ✓ OS Upgrades
- ✓ Software Deployment
- ✓ Free Script Marketplace
- ✓ Managed Reboot Behaviour

Automation

Reduce risk and resource strain

Threats don't take time off, but you can. TOPIA's auto actions enable automatic threat mitigation and response. With auto actions, you can automatically update single assets or entire groups, deploy patches based on severity, and even set scripts to run a network scan with Nmap in response to predefined triggers.

- ✓ Asset Group-based Activities
- ✓ Remedy Actions Scheduling
- ✓ Patching Automation
- ✓ Script Execution Scheduling

- ✓ OS Upgrades Automation
- ✓ Network Scans Automation
- ✓ Audit Log and Tracking
- ✓ Remedy Action Sequencing

vicarius.io