vicarius.io

TOPIA

TOPIA analyzes, prioritizes and protects third-party apps against exploitation.
Manage your organization's security cycle from start to finish and protect more, faster by focusing on the threats that matter most.

0-Day

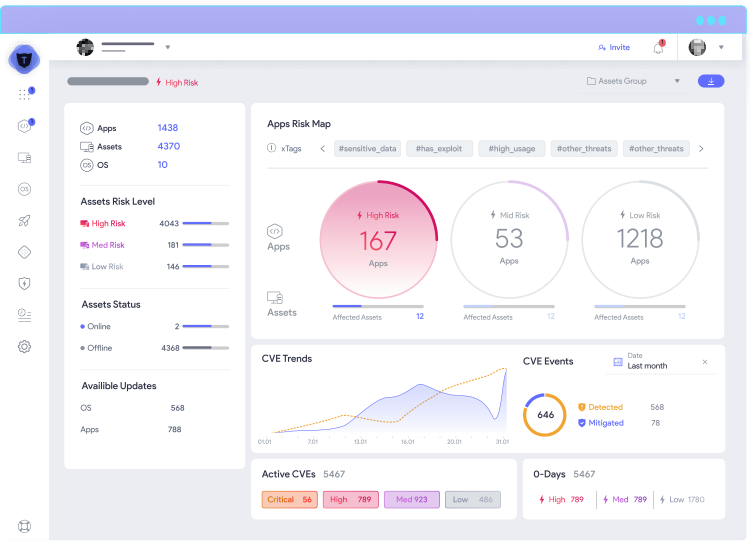
TOPIA's Zero-Day Analysis tool uses predictive analysis to track malware activity and predict incoming attacks. Be informed about potential weaknesses before hackers find them.

xTags™

xTags help prioritize threats using contextual scoring, like prioritization parameters, access authority and activity status, in order to determine the risk level of every application and asset in your organization.

Patchless

With TOPIA's Patchless Protection , vulnerable applications are secured within a force field until the next patch has been prepared, tested, and deployed. Beat the patch gap and stay protected.



01

Analyze

Detect CVEs and binary level threats

TOPIA is the first end-to-end vulnerability remediation solution with the ability to analyze proprietary and niche applications for vulnerabilities without official CVEs, providing full asset visibility and threat intelligence. Its real-time analysis engine identifies CVE and 0-day threats by continuously analyzing third-party software applications.

App Auto Recognition

TOPIA's Auto App Recognition tool detects installed apps across organizational assets and creates a software inventory of their most recent versions.

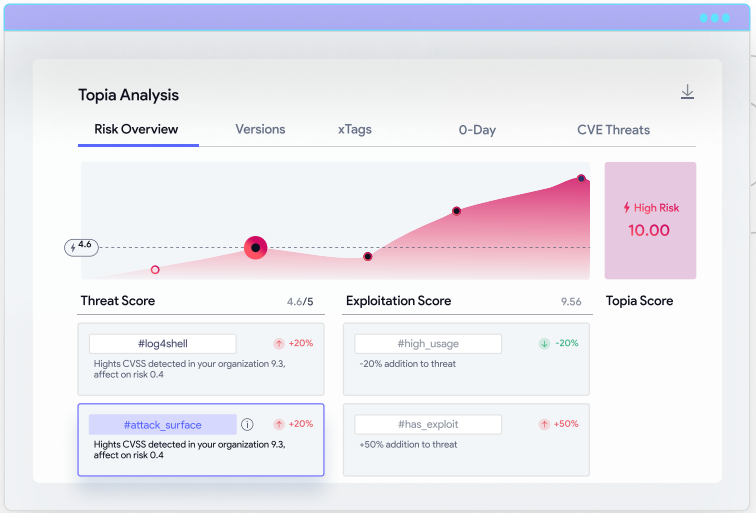
App Threat Analysis

TOPIA's App Threat Analysis tool runs a binary analysis of all third-party apps to detect common vulnerabilities, including zero-day and CVE threats.

Asset Threat Analysis

TOPIA's Asset Threat Analysis tool analyzes active and non-active assets within your organization to determine their overall exploitation and risk level.

Contact us for more details info@vicarius.io



02

Prioritize

Focus on the threats that matter most

An innovative prioritization engine combines the infrastructure context landscape with thousands of data points and 0-days to accurately pinpoint any outstanding risk. TOPIA's prioritization combines threats such as well-known vulnerabilities and 0-days with our proprietary xTags mechanisms, creating a clear-cut picture of immediate risk as a result of both threat and exploitation.

xTags™

TOPIA's xTags™ prioritize all detected threats based on their severity using contextual scoring, identifying the most critical threats your organization faces.

App & Asset Risk Scoring

TOPIA ranks the risk and severity of each app and asset in your organization based on their level of threat and exploitation, providing a focused view of risk.

Prioritization Mapping

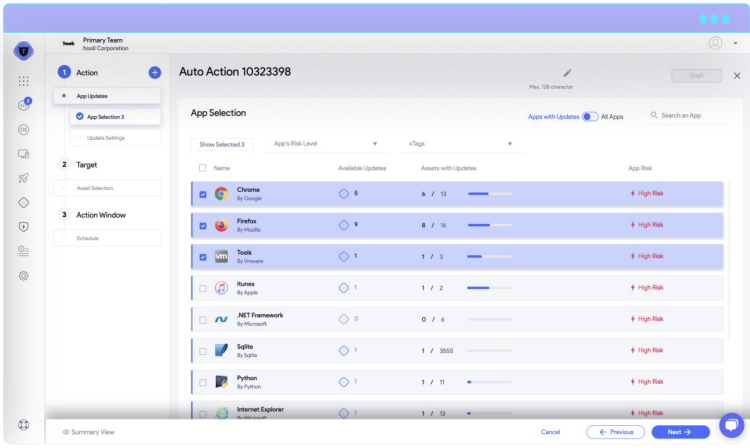
TOPIA maps the potential consequences of a successful exploit within your unique digital infrastructure, so your infosec teams can confidently prioritize risk remediation.

03

Remediate

Deploy updates automatically and remotely

For each threat it analyzes, TOPIA provides a list of recommended actions to reduce risk, enabling you to stay safe and resilient no matter what threat you are confronting. In cases where there is no patch, or you do not wish to upgrade, TOPIA's Patchless Protection will protect you without any downtime or reboot.



Auto Actions

With TOPIA's Auto Actions, you can automate routine updates, deploy patches automatically based on severity, and even set scripts to run anytime in response to triggering factors.

Real-Time Patch Management

TOPIA's Real-Time Patch Management gives you the flexibility to close security gaps or schedule patch installations on Windows, MacOS, and Linux operating systems.

Patchless Protection™

TOPIA's Patchless Protection™ tool secures high-risk apps and blocks incoming exploitation attempts using proprietary in-memory protection.