SIXMAP

Preemptively Mitigate Cyber Risks With
Continuous Exposure Assessments

SixMap runs continuous, comprehensive exposure assessment so you can mitigate risks faster.

Threat actors are deploying AI to automate cyber attacks. While this malicious use of AI is increasing the frequency and velocity of attacks, the underlying techniques are familiar. One of the primary objectives of adversarial AI is to find exploitable risks, such as misconfigurations and high-severity CVEs. To defend against these AI-driven attacks, security teams need advanced technologies to fully automate the fundamentals: asset inventory upkeep, exposure assessments, and risk detection.

SixMap continuously provides complete and accurate data on every asset, exposure, and vulnerability across your organization's digital estate. The exposure assessment process is truly continuous and a new job begins the moment the previous ends. All 65,535 ports are inspected on each asset, every assessment. Customers can select any two assessments to view the delta– every new asset, open port, service, and vulnerability– and quickly see what has changed between those two points in time.

Key Benefits & Business Value

Exhaustive Exposure Visibility
Continuously inspect all 65,535 ports on each asset, every time the assessment procedure runs.

Continuous Insights
Run continuous assessments. Select any two jobs to quickly view every single change in your environment.

Proactive Threat Hunting
View every new exposure to quickly find potentially malicious activity, such as backdoors and data exfiltration.

Simplified Audits & Compliance
Access data on every asset, open port, service, and vulnerability for easy auditing and compliance.

External Exposure Reporting
Easily view the difference between any two points in time (e.g. a quarter, a fiscal year) for easy reporting.

Preemptive Risk Mitigation
Preemptively detect and mitigate critical risks before threat actors can find and target them.

SixMap's Platform: Comprehensive Exposure Assessment

SixMap's exposure assessment runs continuously– a new job begins the moment the previous one ends. All 65,535 ports are inspected on each host so no exposure is left undetected.

Exhaustive Assessments & Continuous Processes

Many legacy exposure assessment tools only check the top 1,000 to top 5,000 ports, leaving hidden risks exposed. SixMap continuously inspects all 65,535 ports on each asset, every job.

Custom Exposure Insights & Simply Diff Analysis

The data for each of SixMap's assessments are logged so customers can quickly see exactly what's changed, down to every open port and service exposure, between any two points in time.

Automatically Structured Data & Exposure Attribution

SixMap's entity-first approach ensures that each asset– plus every downstream data point, like ports, services, and CVEs– is automatically assigned to the entity responsible for protecting it.

Accurate Exposure Data & High-Fidelity Risk Detection

SixMap operates an independent ISP so the discovery and exposure assessment processes are efficient and silent. The asset and exposure data provided is complete and accurate.

> "
> **SixMap has saved us the equivalent of a full-time employee's worth of effort by automating discovery, enumeration, and risk analysis.**
> "
>
> **-Doug Gernat**
> *CISO for the City of Richmond, Virginia*

SixMap delivers the most complete and accurate external view of any public or private organization, showing security teams who they are, what they own, and what they must protect. By closing the gap between what security teams monitor and what adversaries find through reconnaissance, SixMap helps customers mitigate risks before attacks occur. Its strategic mapping ensures no assets are overlooked, while advanced technology pinpoints hosts, exposures, and risks with precision. Born out of national defense and deployed to protect some of the nation's most sensitive networks, SixMap now brings military-grade capabilities to public and private organizations to preemptively stop cyberattacks.

BOOK A DEMO

SIXMAP