

# Bridging the Reconnaissance Gap

*SixMap bridges the gap between what cyber defenders are protecting and what threat actors uncover through advanced reconnaissance.*

Large organizations are made up of many entities: brands, subsidiaries, operating companies, business units, regional divisions, and other components that comprise the broader enterprise. This fragmentation leads to highly complex and dynamic digital estates. It is an ongoing challenge for security teams to understand their organization, what digital assets they must defend, and what risks are currently exposed.

SixMap conducts continuous, fully automated reconnaissance of an organization, in exactly the same way that a sophisticated attacker would. The process begins by mapping out the organization and understanding the structure before beginning network discovery. SixMap's technology finds all hosts across IPv4 and IPv6, then inspects all 65,535 ports on each host every time the assessment is run. All CVE findings are enriched with threat intelligence for simplified prioritization and faster mitigation cycles.

## Key Benefits & Business Value



### Access Data You Can Trust

Get complete, accurate data about your assets and exposures.



### Gain Value Instantly

Get results and value immediately after a zero-touch deployment.



### Save Time & Resources

Save time spent managing exposures and shift focus to other priorities.



### Enable SOC Automation

Send better data to your security stack, improving automated workflows.



### Enhance Security ROI

Improve returns on other tools and processes that rely on accurate data.



### Reduce Cyber Risk

Accelerate remediation cycles, reduce risk, and stay secure.

# SixMap's Solution

SixMap's **preemptive exposure management platform** provides the data security teams need to enhance automation, increase the fidelity of detection, accelerate remediation, and reduce risk.

## Map: Organization Mapping

Map your organization's structure and identify all entities. Each entity acts as a starting point for the discovery procedure, so all assets are automatically assigned to the responsible entity.

## Discover: IPV4 & IPV6 Host Discovery

Discover hosts with high precision across both the IPv4 and IPv6 address spaces. Gain comprehensive data by finding all domains and IP addresses that belong to each entity.

## Assess: Exposure Assessment

Conduct a thorough exposure assessment for all discovered hosts. Inspect all 65,535 ports on each asset, every scan, to uncover exposures on non-standard ports and other unknown risks.

## Prioritize: Risk-Based Prioritization

Detect hidden CVEs and easily prioritize vulnerabilities for remediation with threat intelligence data. Understand which CVEs are exploited in the wild and which groups are exploiting them.

//  
**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