



# Automated Cyber Defense

SixMap introduces the next evolution in  
**Continuous Threat Exposure Management**



## Without any setup, agents, or privileges:

- ✓ Discover all Internet-facing assets across your extended enterprise solely from your enterprise's name
- ✓ Identify imminent threats to the network through validated vulnerability assessments and global threat actor intelligence
- ✓ Defend your enterprise with precise actions delivered to the security operations center for remediation or leverage SixMap's auto-fix capabilities

## Customer engagements demonstrate transformational improvements:

- ✓ **Automate 99.9%** of enterprise and network coverage
- ✓ **Reduce up to 99.9%** of actionable alerts
- ✓ **Use measurable results** to efficiently and effectively stop threats before a breach



## AUDITABLE RISK MITIGATION

When you use SixMap to take actions that stop specific adversaries and attacks, you obtain continuous validation of your remediation efforts and return on investment with evidence-based, auditable results over time, including quantified proof of averted losses.



## IMPROVED OPERATIONAL EFFICIENCY

By streamlining the risk reduction process to demonstrable threats, SixMap force multiplies your security team's ability to achieve desired security outcomes.

# Comprehensive Visibility and Intelligent Action

Start with Enterprise Name Only

Comprehensive Enterprise, Network, and Vulnerability Discovery



Contextual Exposure, Exploit, and Threat Intelligence

Automated Remediation and Validation

## HOW IT WORKS

With just a company name, SixMap will identify your extended enterprise, networks, and assets. We then enrich this data with contextual information on exposures, threat actors, and risk, pinpointing the most urgent threats and precise actions you can take to stop them.

### Start with Enterprise Name Only

- ✔ Activate SixMap's comprehensive mapping with **no installations or special access** required by just providing your enterprise name.
- ✔ Generate a detailed list of your **entire extended enterprise automatically**, including subsidiaries, acquisitions, and third-party affiliations, globally.
- ✔ Visualize your **organizational structure**, providing clear insights into what you're defending, all automated by SixMap.

### Comprehensive Enterprise, Network, and Vulnerability Discovery

- ✔ Discover **all Internet-facing services and devices**, and identify vulnerabilities and misconfigurations for an in-depth understanding of your extended enterprise's security posture.
- ✔ Identify every Internet-connected asset and device, creating an extensive network map across IPv4, IPv6, and enumerating services on **all 65,535 ports**.
- ✔ Discover **vulnerabilities through interactive analysis** that cannot be detected with service detection nor banner grabbing alone.

### Contextual Exposure, Exploit, and Threat Intelligence

- ✔ Gain near real-time **global threat intelligence** about threat actor activity worldwide, including who they are, what they do, and how they do it.
- ✔ Pinpoint **imminent threats** to your enterprise, including the threat actor involved, the exploit to be used, and the targeted network, device, and vulnerability within your enterprise.

### Automated Remediation and Validation

- ✔ Leverage a range of remediation options for **maximum impact with minimal effort**, including auto-fix capabilities that require no action from your teams.
- ✔ Streamline the threat response process by integrating SixMap insights on specific imminent threats with your **Security Operations Center (SOC) tooling via API**.
- ✔ Validate the effectiveness of remediations post-implementation to ensure the fix was implemented properly and to **gather auditable results**.

**Seeing is believing.**  
No setup. No agents.

Immediate Value. Let us show you.

[Get a Demo →](#)



SixMap and the SixMap logo are trademarks or registered trademarks of SixMap and/or its affiliates. To view a list of trademarks, please visit: <https://www.sixmap.io/terms/>.

sixmap-inc

