SIXMAP

WHITEPAPER

SixMap Automated Cyber Defense: Business Justification for Enterprise Decision Makers

Executive Summary

Enterprises today are facing a relentless barrage of cyberattacks that evolve in sophistication, with adversaries leveraging advanced technologies like automation and AI. Over 27,000 new Common Vulnerabilities and Exposures (CVEs) were published in 2023,[1] with around 25% rated as critical.[2] Enterprises struggle to keep up, taking an average of 88 days to patch these vulnerabilities[3], while attackers exploit them in mere minutes. This leads to significant financial and operational risks, with the average cost of a data breach due to known, unpatched vulnerabilities reaching $4.17 million.[4]

The SixMap Automated Cyber Defense Platform is designed to address these challenges, delivering continuous visibility, risk prioritization, and supervised automated remediation at scale for your external networks. The platform's unique zero-touch architecture reduces the burden on IT and InfoSec teams while providing comprehensive and continuous coverage of both IPv4 and IPv6 networks. SixMap helps organizations gain full visibility into their internet-facing assets, prioritize the most critical threats, and respond proactively to mitigate risk, all without disrupting network performance and day-to-day operations.

[1] MITRE
[2] NIST
[3] Statistica
[4] IBM Cost of a Global average age in days of cyber vulnerabilities in 2023, by severity Data Breach Report 2023

Customer Challenges

Based on extensive industry discussions, SixMap aims to address the following common pain points faced by enterprise cyber teams as it pertains to their external network defense:

1 Sophisticated Adversaries:

Cyber adversaries, particularly state-sponsored ones, use advanced technologies and resources, making attacks more sophisticated and continuous.

2 Insufficient Visibility:

Enterprises often lack comprehensive visibility into their external attack surface, including subsidiaries, third-party networks, and cloud environments.

3 Alert Overload & Prioritization:

IT teams are overwhelmed by alerts from various security tools, making it difficult to prioritize critical threats.

4 Prolonged Detection & Remediation:

The time lag between vulnerability detection and remediation leaves organizations exposed to attacks for extended periods.

5 Resource-Intensive Security Operations:

Integrating and managing multiple security tools to form a cohesive security strategy is time-consuming and labor-intensive.

6 High Cyber Insurance Premiums:

Enterprises are unable to negotiate lower insurance premiums due to inaccurate security assessments or unmitigated vulnerabilities and worse case they are not getting full insurance coverage due to a lack of full enterprise and network visibility.

7 Third-Party & M&A Risk:

Companies struggle to evaluate the security posture of third-party vendors and M&A targets before integrating them into their networks.

8 Regulatory Compliance:

Maintaining continuous visibility of external attack surfaces is critical for compliance with regulations like SOX, GDPR, and SEC rules.

9 Shadow IT Risks:

Unapproved or rogue IT assets on the network can introduce hidden vulnerabilities, increasing risk across the organization.

SixMap Solution Overview

SixMap is built to help enterprises overcome these challenges by automating and simplifying critical security processes:

Enterprise Discovery & Asset Mapping

SixMap automatically maps your entire global enterprise, including subsidiaries, acquisition targets, and third-party vendors. The platform scans all internet-facing assets, covering both IPv4 and IPv6 networks. This ensures no aspect of your digital footprint is missed, reducing shadow IT risks and providing a complete, accurate inventory of your attack surface continuously at scale.

Risk Assessment

SixMap continuously scans all 65,535 ports on every internet-facing device, identifying exposed services and potential vulnerabilities. The platform supports publicly available and third party vulnerability detection modules, enabling organizations to tailor risk assessment to their specific needs.

Threat Prioritization

Using real-time global threat intelligence, SixMap correlates discovered vulnerabilities with imminent threats. By integrating data from both public and proprietary sources, the platform prioritizes vulnerabilities based on their likelihood of being exploited with active exploits being most critical. The continuous and comprehensive mapping of the extended enterprise and its network allows these vulnerabilities to be contextualized in real time.This allows your security teams to focus on the highest-risk vulnerabilities, enabling quicker and effective remediation.This capability also provides a more efficient use of the cyber response teams time and efforts.

Proactive, Automated Response

SixMap enables supervised, automated remediation, reducing the time between detection and action. The platform can automatically push firewall rules, filter malicious traffic, and even apply remote patches for critical vulnerabilities (e.g., RCE) with customer approval. This ensures a rapid, proactive response to emerging threats without burdening IT teams.

Competitive Differentiation

✓ Zero-Touch, Fully Automated Deployment

Unlike traditional tools that require manual configuration or agent installation, SixMap operates with a zero-touch, fully automated architecture. This minimizes disruption during deployment and dramatically reduces the operational burden on already stretched IT resources. Just provide your company name, and SixMap begins its real-time network monitoring and defense.

✓ Golden Bonsai & Computational Mapping Technology

SixMap's proprietary **Golden Bonsai** and **Computational Mapping** technologies enable highly efficient and scalable scanning across both IPv4 and IPv6 networks. These technologies reduce the time and resources required to maintain an accurate, continuously updated map of your extended enterprise including subsidiaries, acquisitions, third parties and associated networks , compared to traditional brute-force discovery and scanning methods. **Continuous mapping at scale** will be the only way to ensure your organization stays ahead of emerging threats.

✓ Comprehensive Coverage of All Ports at every scan

Unlike other solutions that only scan a subset of ports or provide results over extended periods, SixMap scans all 65,535 ports for every internet-facing asset at ultra-high speed at every scan without impacting the network performance. This ensures that no services or vulnerabilities are missed, delivering a more comprehensive risk assessment than other tools.

✓ Real-Time Threat Intelligence Integration

SixMap integrates both public and private global threat intelligence sources, to provide real-time insights into which vulnerabilities are being actively exploited globally. This allows for the prioritization of the most imminent threats, ensuring optimal use of your security resources..

Business Impact

By adopting SixMap, enterprises can address key security and operational challenges while realizing significant business benefits:

1 Reduced Operational Costs

SixMap automates time-consuming processes such as asset discovery, vulnerability assessment, and remediation, freeing up valuable resources and reducing the need for specialized, manual intervention. This enables IT teams to focus on strategic initiatives instead of daily firefighting.

2 Improved Security Posture

SixMap provides full, continuous visibility into your external attack surface, helping to identify and prioritize critical vulnerabilities before they can be exploited. With faster detection and remediation, enterprises can significantly reduce their risk of costly breaches.

3 Lower Cyber Insurance Premiums

SixMap's ability to reduce false positives and accurately assess the security posture of your organization in a continuous manner enables you to negotiate lower cyber insurance premiums. By providing continuous, evidence-based security data, SixMap helps demonstrate to underwriters that your organization is proactively managing and mitigating risks.

4 Compliance & Regulatory Assurance

SixMap simplifies regulatory compliance by ensuring continuous visibility into your internet-facing assets and providing detailed reports that help satisfy legal and policy mandates like SOX, GDPR, and SEC rules.

5 M&A and Third-Party Risk Management

SixMap provides non-intrusive, automated assessments of third-party vendors and M&A targets, allowing enterprises to fully understand their cybersecurity risks before integrating them into their networks. This helps streamline M&A due diligence and reduce the risk of supply chain vulnerabilities.

Conclusion:

A Smarter, Faster, and Proactive Cyber Defense Solution

As cyber threats become more sophisticated and the stakes of a breach grow higher, enterprises need a cybersecurity solution that can keep pace. **SixMap Automated Cyber Defense Platform** provides comprehensive, continuous visibility, real-time threat prioritization, and automated remediation—all with a zero-touch architecture that reduces operational overhead.

By choosing SixMap, your organization will be better equipped to defend against modern threats, reduce operational costs, improve regulatory compliance, and strengthen your overall security posture.

Schedule a demo today to see how SixMap can help transform your organization's approach to cybersecurity.

SIXMAP