WHITEPAPER

SixMap Automated Cyber Defense and Its Network Security Implications

Assess Risk, Prioritize Threats, and Proactively Respond with SixMap

SIXMAP

EXECUTIVE SUMMARY

Preventing computer network exploitation is a major challenge for most large enterprises. Adversaries continuously evolve their tactics, techniques, and procedures, finding new ways to penetrate networks, disrupt business-critical systems, and steal confidential data. At the same time, detecting, prioritizing, and patching vulnerabilities is a resource-intensive, time-consuming proposition. Over 27,000 new CVEs were published in 2023[1] and about 25% of them had a CVSS score of 7.0 or higher.[2] **Most InfoSec and IT teams are simply overwhelmed. In fact, the average time to patch a critical vulnerability is 88 days.[3] Not surprisingly, 30% of security breaches are linked to network-based attacks, and 93% of network-based attacks leverage known but unpatched CVEs.[4] These breaches are also damaging and expensive for the business; the average total cost of a data breach arising from a known but unpatched vulnerability is $4.17 million.[5]**

The SixMap Automated Cyber Defense Platform is purpose-built to force-multiply enterprise IT and InfoSec teams and accelerate their ability to gain continuous visibility of their Internet-facing assets across IPv6 and IPv4 networks at scale; assess risk, prioritize threats, and respond with minimal customer involvement. **SixMap is the industry's first and only zero-touch capability that enables automated, continuous, and comprehensive enterprise enumeration, network risk visibility, threat based prioritization, and supervised proactive response, in a single, unified cyber platform.**

The SixMap platform functionality includes:

- **Enterprise discovery** to provide a complete picture of your global organizational makeup
- **Asset discovery** to identify all your Internet-accessible resources
- **Risk assessment** to uncover potential security vulnerabilities
- **Threat prioritization** to help you align mitigation efforts with risk potential
- **Supervised proactive response** to remote remediate certain types of security vulnerabilities (i.e. remote code execution) with prior approval from the customer team.

SixMap is powered by a new **computational mapping technology** that overcomes the inefficiencies and performance constraints of conventional external attack surface and vulnerability management solutions. The SixMap platform enables defenders to execute network security workflows at unmatched speed and scale, helping to stop threats faster. The platform looks at the enterprise and network the same way an adversary would.

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

The Challenge: Keeping Pace with the Constantly Evolving Threat Landscape

Detecting vulnerabilities and managing threats is a significant challenge for today's dynamic enterprises. **Adversaries routinely take advantage of both gaps in continuous comprehensive visibility and delays in patching vulnerabilities to exploit computer networks.** Contemporary enterprise networks are vast, complex, and inherently difficult to defend; they are composed of multiple independent networks attached to a multifaceted enterprise, include hybrid and multi-cloud environments, and employ a mix of IPv4 and IPv6 address schemes, which make it difficult for defenders to obtain continuous and complete network visibility across their Enterprise.

In addition, many teams are short-staffed and most SecOps teams are inundated with security alerts. Pinpointing, prioritizing, validating, and fixing vulnerabilities is a time-consuming proposition; the average time to patch a critical vulnerability is approximately 3 months.[6] These challenges have resulted in crippling ransomware attacks in addition to supply chain attacks becoming increasingly common.

The SixMap Solution:

The SixMap Automated Cyber Defense Platform was specifically conceived to overcome the limitations and inefficiencies of traditional threat management systems and practices. SixMap employs unique proprietary technology, first to gain complete visibility for the entire public-facing digital estate for the extended enterprise across all geographies and corporate entities, then to prioritize threats helping to identify and remediate the greatest risks to your business in a continuous and timely manner. SixMap's solution helps you meaningfully strengthen your security posture by accelerating remediations. Actionable insights let you address vulnerabilities before adversaries exploit them and do irreparable harm to your business and proactive response functionality lets SixMap automatically resolve certain types of acute security concerns in coordination with your security response team.

The SixMap platform is designed from the ground up to be nonintrusive and effortless to deploy, administer, and scale. The solution is based on a zero-touch architecture and delivered as a fully managed service hosted and operated on SixMap owned and managed infrastructure for ultimate simplicity, extensibility, and agility. SixMap does not require agents that might impair network performance or complicate ongoing IT operations and it does not require privileged access to any of your systems.

To get started, simply tell us the name of your business. We take it from there. With SixMap you can leverage automation to:

- **Enumerate** your extended enterprise
- **Discover** all Internet-exposed devices and assets
- **Identify** network services and vulnerabilities—including new threats not yet published in the NVD
- **Prioritize** risk by tracking global threat actors and correlating attacks with exposure to focus mitigation efforts
- **Respond** to demonstrable threats

The SixMap Platform

The SixMap Automated Cyber Defense Platform is a tightly integrated, holistic solution combining enterprise and asset discovery, risk assessment, threat prioritization, and proactive response functionality.

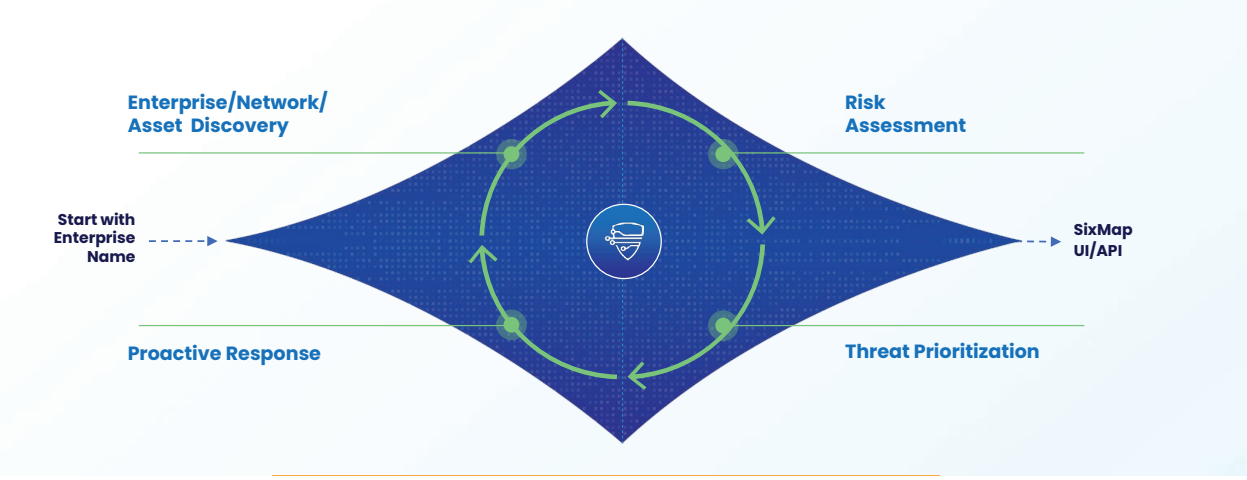

Figure 1. SixMap Automated Cyber Defense Platform

[6]Statistica

Enterprise/Network Discovery

SixMap has demonstrated both a false positive (FP) and false negative (FN) rate of < 0.001% based on ground truth tests on large Fortune 100 and United States Government (USG) organizations and their networks as it pertains to Enterprise Discovery and network mapping.

Traditional network mapping offerings search Internet records such as WHOIS and RDAP in order to both build a picture of an enterprise and find its networks—this approach is inherently flawed because Internet records were never designed to be enterprise records or to build a map of the enterprise itself. SixMap is different in that we build a comprehensive picture of the enterprise using a broad spectrum of Internet data from the World Wide Web, corporate, and government records. We collect this data both from open sources, and commercial intelligence products, such as business reconnaissance data. We use a proprietary fusion process to combine all of the different data sources first together and then with traditional Internet records and historical passive and active Internet-wide measurement surveys. The plethora of WWW and enterprise data sources we incorporate contain a large number of records—at the same time there are a large number of Internet records—these all need to be fuzzy searched, tokenized, and cross-referenced. In addition, today's enterprise is complex and dynamic, sometimes containing hundreds or thousands of subsidiaries and associated entities as a part of the extended enterprise. As you can imagine, our approach requires collecting and processing massive amounts of data and was originally thought to be impossible just to produce initial results, let alone results with nearly no false positives and negatives. We accomplish this task by using our proprietary computational mapping technology to reduce the "hardness" or theoretic complexity of "work" required by several orders of magnitude compared with how traditional approaches would try to solve this problem, using brute force methods that either impact network performance or alternately discover only a subset of the extended enterprise networks. We also use our technology to enable parallelized offline computation wherever possible which reduces both real world "wall-clock" time and the workloads required to be performed external to SixMap High Performance Computing infrastructure.

Asset Discovery

Once we discover all the entities in an enterprise (e.g., subsidiaries) and their associated Internet records (e.g., WHOIS & DNS), we then turn to identifying the public Internet-accessible network assets via active measurements. SixMap is the only solution in the market that can perform a full scan of all 65,535 ports for every Internet-facing network at every scan, at ultra-high speed, identifying potential attack vectors other tools miss.[7]

[7]Some vulnerability assessment solutions only interrogate a subset of ports, scanning only officially assigned and widely used ports. Other solutions scan the full range of ports, but only over an extended period, not providing timely results.

We actively measure and model the Internet using SixMap-owned and operated bi-coastal high performance computing (HPC) data centers. Our HPC infrastructure is connected directly to the Internet backbone with a SixMap-owned and operated in-house network using Tier-1 ISP grade technology. (i.e.~ 1 Tbps of switching capacity, designed with numerous 100 Gbps switching components and 10 Gbps 1510 nm single mode fiber lines for redundancy and reliability.)

We identify all of the autonomous systems and BGP prefix announcements associated with the enterprise by fuzzy matching on the global BGP routing table, including contextual information such as RPKI data, from the perspective of Tier 1 ISPs. In addition, we identify network blocks that have been sub-allocated to the organization from other ISPs—again using contextual analysis on the blocks. We also leverage near-real-time global passive DNS data and global active mapping data to identify all the subdomains associated with the entity.

We scan all of these networks using our proprietary computational mapping technology that builds a model of the network in real time as the scan is happening. Once again, we use computational mapping to reduce the difficulty of the problem using "real-time" modeling and "offline" computation, ultimately reducing the search space from billions of IP/port tuples[8] down to just thousands. The concept is simple but hard to execute—learn about the network using as few measurements as possible—use the model to predict what the network looks like—and then validate the model with active probing. Theoretically this approach should produce inferior results to traditional ASM that uses exhaustive probing to discover IPs and ports. In practice, our approach achieves something that is counterintuitive; it finds more hosts and open ports while sending fewer probes. This characteristic is attributable to the fact that traditional exhaustive probing presents a conundrum; you can either scan fewer ports, overload the network with traffic, or scan at a much lower frequency. SixMap overcomes this problem because our mapping approach is orders of magnitude more efficient.

Risk Assessment

Once we capture the IP/port tuples, we interrogate the open ports with two types of risk measurements. First, we run service version number (SVN) detection modules, second, we run native vulnerability assessment (NVA) modules. Our SVN modules discover vulnerabilities by converting SVNs to CPEs to CVEs. Conversely, our NVA modules do not run SVN or CPE detection, and instead they directly test for the vulnerability. NVA can run in detection or validation mode, in detection mode the platform detects the vulnerability without running the exploit, in validation mode the exploit is run and exploitation is validated. While not for all customers, validation mode is a game-changer for red teams, and breach and attack simulation use cases.

[8] A tuple uniquely defines a network connection. For example, a 5-tuple includes a source IP address, source port number, destination IP address, destination port number, and the protocol in use (TCP or UDP).

We have a set of SVN and NVA modules that we run by default, however, the SixMap platform enables customers to run open-source SVN and NVA modules or customer-supplied modules. This unique functionality is possible due to the modular design of our mapping engine, the power of our HPC and ISP infrastructure, and the efficiency of our computational mapping approach.

Threat Prioritization

After the SixMap platform enumerates all vulnerabilities, it indexes them and fuses this index against the latest global threat intelligence to prioritize which vulnerabilities are most likely to be exploited by an adversary. SixMap fuses open-source and closed-source threat intelligence from both United States Government and commercial threat intelligence feeds. We also pull the latest Exploit Prediction Scoring System (EPSS) rating for each vulnerability.

We sort vulnerabilities into three main categories: observed exploitation, high EPSS, and all other CVEs. Our observed exploitation category only includes vulnerabilities with confirmed exploitation by a threat actor sorted by recency. Our EPSS category includes vulnerabilities likely to be exploited in the next 30 days, but where we or one of our threat intelligence partners have not yet observed exploitation. And the last category contains all other vulnerabilities. The number of vulnerabilities in each category increases exponentially while risk of exploitation decreases exponentially; therefore, remediating vulnerabilities in the order presented by the SixMap platform provides an optimized return on investment for network security operators.

Proactive Response

The SixMap platform provides a spectrum of action to respond to threats with increasing levels of automation. First, you can use SixMap to retrieve and push firewall rules matching the exploits to DPI (deep packet inspection) capable IPS (intrusion and prevention system) on your network. Second, SixMap can filter Internet traffic while allowing local traffic so that adversaries cannot reach the service but customer assets on the same network still can. Third, if the exploit grants RCE and admin privileges, SixMap can use the exploit to obtain RCE on the device and then run the patch as admin. These actions are conducted with a human-supervised process that is coordinated with the customer and ownership of the assets is validated using cryptography.

Evaluating Third-Party Cyber and M&A Readiness with SixMap

With SixMap you can non-intrusively evaluate the internet-facing security posture of any third-party organization, without their knowledge or participation. SixMap does not rely on special-purpose endpoint software to scan systems. And we don't require admin privileges. We simply probe Internet-facing assets just like an external threat actor would, trying to uncover potential security vulnerabilities.

You can leverage SixMap during M&A investigations to identify exposure and assess potential remediation expenses. We can help you improve due diligence efforts by better understanding the total cost of acquiring and assimilating a third-party.

You can also use SixMap to examine the external security posture of the suppliers and business partners your company depends on to produce goods and deliver services. A chain is only as strong as its weakest link. If one of your critical suppliers or service providers is hit by a cyberattack, your business could suffer as well.

Conclusion and Next Steps

Cyberattacks are a major concern for enterprises today. It takes over 88 days for customers to patch a known critical vulnerability[9] on average but just 22 minutes for adversaries[10] to exploit new vulnerabilities. This asymmetry is a problem; it is not surprising that 93% of network based attacks are from known vulnerabilities.

SixMap helps you dramatically improve the speed of your network security team, to strengthen your security posture, and beat the race with the ever-evolving threat landscape. The platform provides unprecedented visibility into your external attack surface and helps you speed up responses and accelerate risk reduction, all with our zero touch architecture.

With SixMap Automated Cyber Defense Platform, you will

- Get full visibility to your extended enterprise including subsidiaries, third parties, acquisition targets etc.
- Increase visibility into internet-facing IT assets, applications & services
- Identify weaknesses across devices, apps, user activities i.e. ghost IT
- Pinpoint vulnerabilities with a higher risk of exploitation
- Reduce business costs by proactively mitigating attack vectors for attack prevention
- Identify and reduce regulatory risks..to ensure compliance with legal/policy/regulatory mandates
- Avoid business and system downtime through enhanced/improved business application & service availability

Want to discover how SixMap can help your company improve cyber readiness? Schedule a call and demo today. It all starts with just the company **name - come find out how SixMaps zero touch, automated network defense solution can help transform your security posture.**

[9]Statistica
[10]bleepingcomputer