RESEARCH REPORT

SIXMAP

ENERGY SECTOR EXPOSURE ASSESMENT

A comprehensive evaluation of 21 of the leading energy providers in the U.S.A. to understand security posture, identify systemic risks, and provide valuable insights to security leaders within the energy industry.

TABLE OF CONTENTS

METHODOLOGY

The goal of this project is to understand the cybersecurity posture of large organizations in the energy sector, identify potential trends that may indicate systemic risk, and provide data-based guidance to security leaders at other organizations within the industry.

To conduct this research, SixMap assessed the external exposures of 21 of the leading energy providers in the U.S.A. SixMap examined all domains and IP addresses, across both the IPv4 and IPv6 spaces, associated with each organization, as well as the ports and services exposed on each asset. For completeness and accuracy of data, all 65,535 ports were inspected.

This research did not engage in any intrusive or harmful activity. Only publicly available data obtained from Internet-facing systems was used for the purposes of this research. As such, this external vantage point cannot see internal mitigating controls that would minimize the damage in the event of attack or exploitation.

SixMap is uniquely positioned to collect and analyze this dataset for several reasons. First, SixMap owns and operates an Internet Service Provider (ISP), which enables exposure assessments to run in an efficient way that provides comprehensive data without causing latency, degrading service response, or creating noise on the networks of the organizations under evaluation.

Second, SixMap uses an innovation called Computational Mapping to enable precise host discovery across the IPv4 and IPv6 address spaces. While many organizations are certain they do not have any IPv6 assets, the discovery process routinely finds IPv6 addresses in use for almost every large organization assessed.

Finally, SixMap inspects all 65,535 ports on each asset, every scan. This provides more complete data and uncovers many exposed services that would not be detected through typical tooling that only checks the top 1,000 to 5,000 most commonly used ports.

EXECUTIVE SUMMARY

As a major component of American critical infrastructure, the energy industry in the United States is highly targeted by both state-sponsored and financially-motivated cyber threat groups. Energy sector enterprises face an increasingly hostile threat landscape and must therefore pay close attention to all the exposures that could be uncovered and targeted by bad actors.

Among the 21 energy sector organizations evaluated for this research project, SixMap identified 39,986 hosts with a total of 58,862 services exposed to the Internet. Approximately 7% (3,910) of all exposed services are running on non-standard ports beyond the top 5,000 most commonly used ports. These 7% of exposures represent potential blind spots, as non-standard ports fall outside the scope of traditional attack surface management and vulnerability management tools.

SixMap found a total of 5,756 vulnerable services with CVEs across all exposures. Many CVEs were detected numerous times. This is true in two ways: several instances of the same CVE within the same organization's environment and several detections of the same CVE in the external attack surfaces of multiple different organizations.

Of the 5,756 CVEs detected, 377 are known to be exploited in the wild, meaning the presence of those CVEs introduces a serious risk and high likelihood of exploitation.

There are 43 different CVEs common to 45% or more of the organizations in the sample group, potentially representing systemic risks for the energy sector.

A total of 304 vulnerable services (231 unique CVE IDs) are running on non-standard ports. 21 of those CVEs are known to be exploited by specific threat groups. This may represent a major challenge for the energy sector, as many industry-standard exposure management products only scan the top 5,000 most common ports by default. If a vulnerable service is running on a non-standard port, it would not be detected by these traditional tools, leaving a high-risk CVE invisible to the security team.

KEY RECOMMENDATIONS:

- **Regularly scan all 65,535 ports to uncover vulnerable services on non-standard ports.**
- **Ensure vulnerability management routinely updates vulnerable exposed services.**
- **Prioritize vulnerabilities based on risk severity and known exploitation activity.**
- **Gain visibility on IPv6 assets to avoid unknown assets from introducing serious risk.**

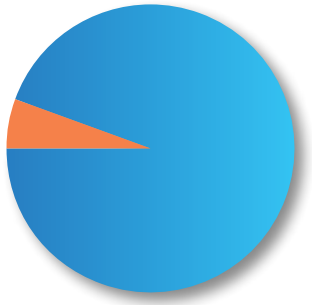
OVERVIEW OF FINDINGS

HOSTS

Total Number of Hosts: **39,986**

Average Number of Hosts Per Organizations: **1,904**

Average Number of IPv6 Hosts Per Organization: **107**



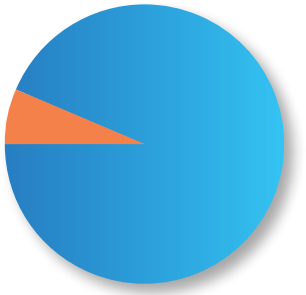
ADDRESSES IN IPv4 VS IPv6 SPACE

SERVICES

Total Exposed Services: **58,862**

Total Exposed Services on Non-Standard Ports: **3,910 (7%)**

Average Exposed Services On Non-Standard Ports Per Org: **186**



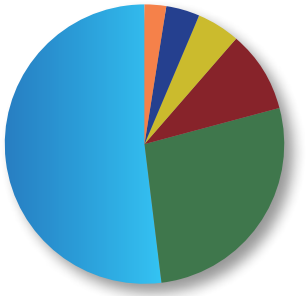
STANDARD VS. NON-STANDARD PORTS

VULNERABILITIES

Total CVEs Found: **5,756**

Total CVEs Tied to Threat Actors: **377 (6.6%)**

Total CVEs on Non-Standard Ports: **304**



DISTRIBUTION OF CVES BY SERVICE

HIDDEN EXPOSURES

EXPOSED SERVICES RUNNING ON NON-STANDARD PORTS

SixMap identified a grand total of 58,862 open ports with services exposed to the Internet across the 21 energy organizations assessed. A total of 3,910 services, or about 7%, were running on non-standard ports that fall outside of the top 5,000 most common ports. This may be an area of risk across the industry, as standard tools typically inspect only a small subset of ports, leaving some services invisible to security and vulnerability management teams.

Below is an overview of the services found running on non-standard ports.

HYPERTEXT TRANSFER PROTOCOL (HTTP)

Hypertext Transfer Protocol (HTTP) is the standard protocol for transmitting web pages and data between web browsers and servers. The standard port for HTTP is port 80.

- Total of 245 instances of http running on non-standard ports
- Sample Non-Standard Ports Found:
  Port 8172 (117 instances)
  Port 65503 (22 instances)
  Port 65504 (22 instances)
  Port 6363 (8 instances)
  Pot 10443 (4 instances)

REAL-TIME STREAMING PROTOCOL (RTSP)

Real-Time Streaming Protocol (RTSP) is used to control streaming media servers for real-time audio and video delivery. The standard port for RTSP is port 554.

- Total of 119 instances of rtsp running
- Sample Non-Standard Ports Found:
  Port 55402 (11 instances)
  Port 55401 (11 instances)
  Port 55403 (10 instances)
  Port 55404 (10 instances)
  Port 10558 (9 instances)

SECURE SHELL PROTOCOL (SSH)

Secure Shell (SSH) provides encrypted remote access and secure command-line communication between networked computers. The standard port for SSH is port 22.

- Total of 16 instances of ssh running on non-standard ports
- Sample Non-Standard Ports Found:
  Port 232 (4 instances)
  Port 18765 (3 instances)
  Port 252 (2 instances)
  Port 7822 (2 instances)
  Port 56383 (2 instances)

SIMPLE MAIL TRANSFER PROTOCOL (SMTP)

Simple Mail Transfer Protocol (SMTP) is the standard protocol for sending and routing emails between mail servers. The standard port for SMTP is port 25.

- Total of 12 instances of smtp running on non-standard ports
- Sample Non-Standard Ports Found:
  Port 26 (12 instances)

MEMCACHED PROTOCOL (MEMCACHED)

Memcached is a high-performance, distributed memory caching system used to speed up web applications by reducing database load. The standard port for Memcached is port 11211.

- Total of 4 instances of memcached running on non-standard ports
- Sample Non-Standard Ports Found:
  Port 11222 (2 instances)
  Port 22122 (2 instances)

MQ TELEMETRY TRANSPORT PROTOCOL (MQTT)

Message Queuing Telemetry Transport (MQTT) is a lightweight messaging protocol for efficient communication in IoT and low-bandwidth networks. The standard port for MQTT is port 1883.

- Total of 1 instance of mqtt running on non-standard ports
- Sample Non-Standard Ports Found:
  Port 8883 (1 instance)

TRANSMISSION CONTROL PROTOCOL - WRAPPED (TCPWRAPPED)

Tcpwrapped indicates that a service is protected by TCP Wrapper, a host-based access control system for network services.

- Total of 45 instances of tcpwrapped running on non-standard ports
- Sample Non-Standard Ports Found: Port 8013 (12 instances), Port 49152 (6 instances), Port 6556 (4 instances), Port 8020 (2 instances), Port 5227 (1 instance)

HYPERTEXT TRANSFER PROTOCOL - PROXY (HTTP-PROXY)

An HTTP proxy acts as an intermediary between a client and web server, forwarding requests and responses while optionally filtering or caching content. The standard port for proxied HTTP is port 8080.

- Total of 40 instances of http-proxy running on non-standard ports
- Sample Non-Standard Ports Found: Port 8020 (35 instances), Port 8015 (2 instances), Port 8899 (1 instance), Port 7563 (1 instance), Port 11388 (1 instance)

UNIVERSAL PLUS AND PLAY PROTOCOL (UPNP)

Universal Plug and Play (UPnP) allows networked devices to automatically discover and communicate with each other for seamless connectivity. The standard port for UPNP is port 1903.

- Total of 36 instances of upnp running on non-standard ports
- Sample Non-Standard Ports Found: Port 10100 (10 instances), Port 10200 (10 instances), Port 10201 (10 instances), Port 6391 (2 instances), Port 6390 (2 instances)

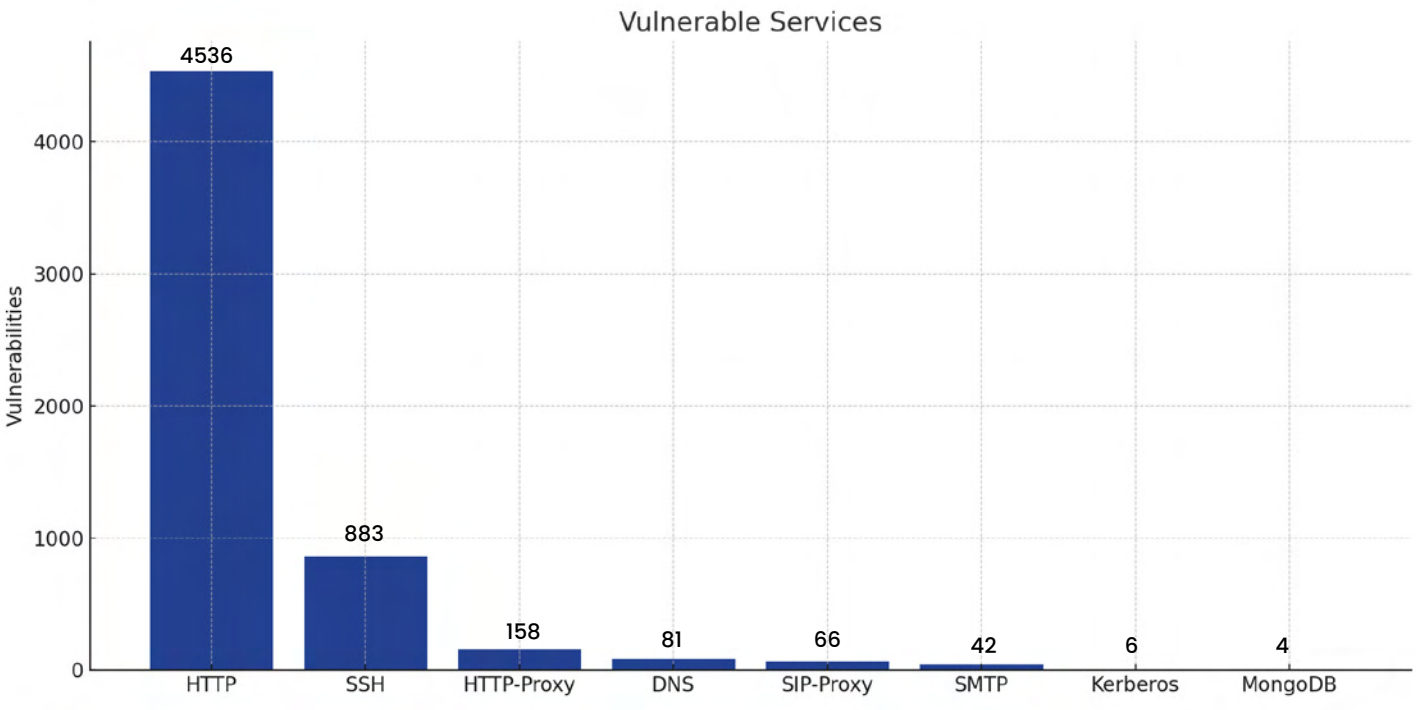
VULNERABLE SERVICES

FREQUENCY OF EXPOSED SERVICES WITH KNOWN CVES

Over the course of this research, SixMap found a total of 5,756 vulnerable services across the 21 energy sector organizations in the sample group. About 76% of these vulnerabilities were with various implementations of HTTP. This is unsurprising, as web services are one of the most common services globally and, by virtue of their purpose, must be exposed to the Internet.

Many other vulnerable services were detected. SSH is of particular risk, as exploiting SSH often results directly in full compromise of a system with the ability to execute commands remotely. Vulnerable DNS services are another area of concern, as there are several attack vectors that bad actors can use to exploit DNS. Other services, such as Kerberos and MongoDB, are also significant risks and should almost always be protected behind a corporate firewall and VPN.

Below is an overview of the 8 services most commonly found to be vulnerable to attack.

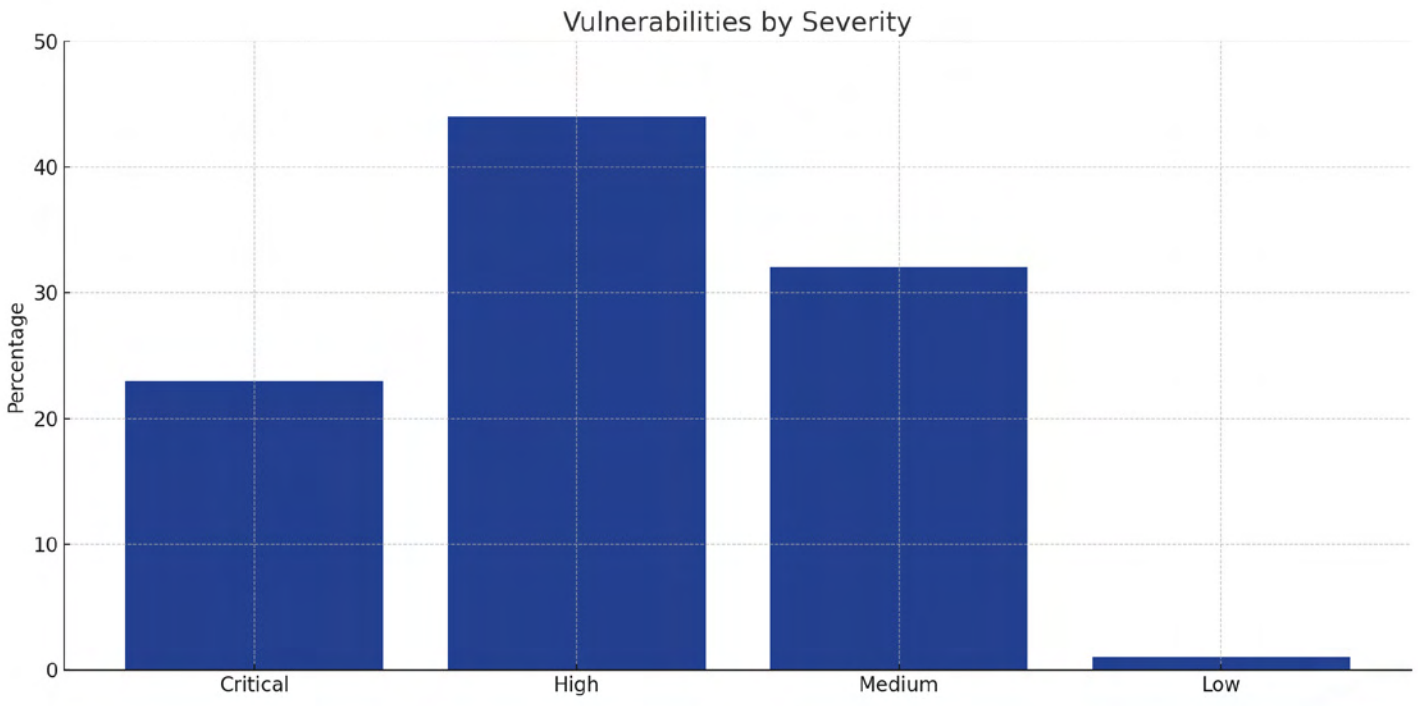


VULNERABILITIES BY SEVERITY

DISTRIBUTION OF VULNERABILITIES DETECTED BY SEVERITY OF RISK

Vulnerabilities, by definition, are a weakness and therefore present a risk. At the same time, some vulnerabilities are more severe than others. The severity of a CVE takes a number of factors into account, including the complexity of exploitation, whether it can be exploited remotely over a network, the impact of exploitation, and much more.

Critical and High severity vulnerabilities represent the most risk of serious disruption to an organization. Below is the distribution of all vulnerabilities SixMap detected by severity rating



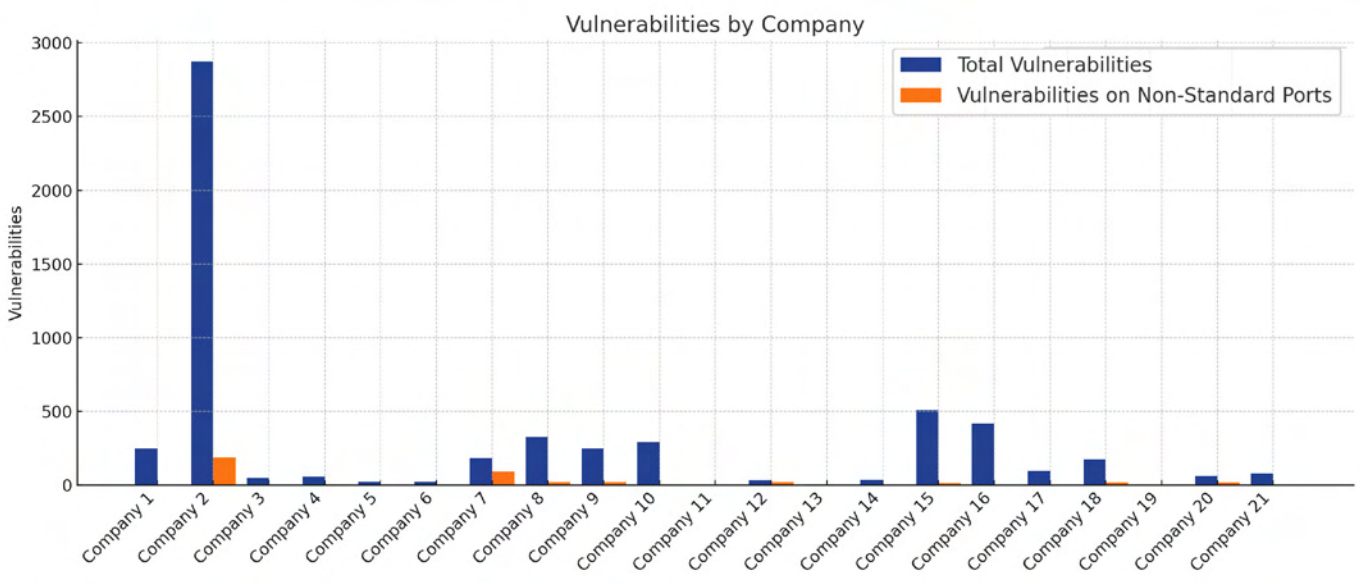
VULNERABILITY DISTRIBUTION

DISTRIBUTION OF CVES ACROSS THE 21 ORGANIZATIONS ASSESSED

SixMap's research found 5,756 vulnerabilities across 21 energy sector organizations assessed, averaging out to 274 vulnerabilities per organization. However, there is wide variance among the sample. One organization has 0 vulnerabilities (and our hats are off to their security team). Three organizations have fewer than 5 vulnerabilities, and seven have fewer than 50.

On the other end of the spectrum, one outlier organization has a staggering 2,875 vulnerabilities in its external attack surface. Many of these vulnerabilities are due to a very old version of Apache web service with 45 known CVEs associated with it. This old web service is running on multiple ports and across multiple hosts. We are left to assume these hosts are shadow IT assets that are unknown to the security team.

It's important to note that many of the vulnerabilities SixMap identified– 405 to be exact, or roughly 7% of all CVEs detected– were with services running on non-standard ports. This suggests a lack of visibility, as many security tools only scan the top 5,000 ports. If a vulnerable service is running on a non-standard port, it may be invisible to security teams, even if they are aware of the host on which the service is running and routinely scan the host for vulnerabilities.



SYSTEMIC RISKS

CVES COMMON TO AT LEAST 45% OF THE ORGANIZATIONS ASSESSED

Known CVEs in services exposed to the Internet, especially those running on non-standard ports, introduce a major risk for any organization. In most cases, these CVEs are left exposed because the security team at the organization is unaware of the CVE. This could be because they are not aware of the host itself, and thus are not monitoring it for CVEs, or they're unaware that the service is running on the host, and thus do not have visibility on the vulnerable service.

SixMap found 43 unique CVEs that were present in the external attack surfaces of at least 10 of the 21 (45%) energy sector organizations evaluated. This suggests potential systemic risk to the industry. If a single vulnerability could be exploited across more than half of the industry's largest enterprises at once, it could be an industry-disrupting event.

The sample list below is only 4 of the 43 CVEs that are common to 10 or more organizations. See the appendix for a full list of all 43 unique CVEs that were common to 45% of the sample.

CVE-2023-38408

Frequency: 16 companies (76.19%)
Service: SSH
Severity: CRITICAL
Known Threat Actors: Silent Chollima
Found on Ports: 22, 70, 722, 2022, 2200, 2222, 2255, 5658, 7822, 21098, 41094

CVE-2024-38476

Frequency: 16 companies (76.19%)
Service: SSH
Severity: CRITICAL
Known Threat Actors: Silent Chollima
Found on Ports: 22, 70, 722, 2022, 2200, 2222, 2255, 5658, 7822, 21098, 9090

CVE-2020-15778

Frequency: 16 companies (76.19%)
Service: SSH
Severity: HIGH
Known Threat Actors: None
Found on Ports: 22, 70, 722, 2022, 2200, 2222, 5658, 7822, 21098, 41094

CVE-2024-38472

Frequency: 11 companies (52.38%)
Service: HTTP
Severity: HIGH
Known Threat Actors: None
Found on Ports: 80, 81, 86, 90, 91, 92, 96, 443, 8000, 8001, 8002, 8007, 8080, 8081, 8088, 8089, 8090, 8091, 8092, 9090

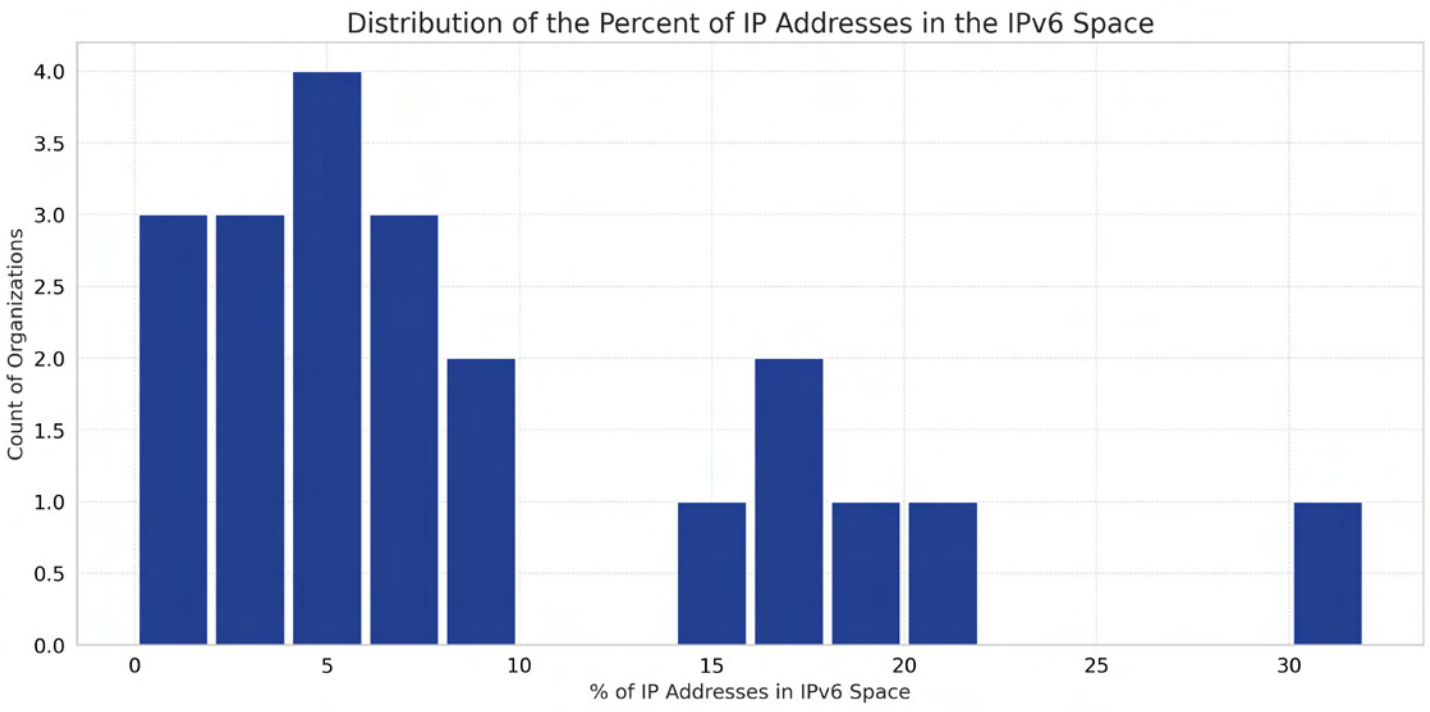
IPV6 EXPOSURE

OVERVIEW OF IPV6 ADDRESSES IN USE AMONG SAMPLED ORGANIZATIONS

Security leaders are often under the impression that they do not have any IPv6 assets. However, SixMap regularly finds IPv6 in use for most large organizations. This experience proved to be true for the energy sector, as every single one of the 21 organizations evaluated has at least one IPv6 address in use.

In total, there are 2,253 IPv6 addresses in use among the sampled organizations, which is about 6% of all the IP addresses discovered over the course of this research. This averages out to roughly 107 IPv6 assets per organization, though there is wide variance.

On average, each organization has about 9% of their IP addresses in the IPv6 space. 7 organizations have at least 14% of their hosts on IPv6 and one has more than 30% on IPv6. Because traditional exposure management tools cannot discover IPv6 hosts, and therefore do not monitor or assess them for vulnerabilities, this may be an area of significant risk.



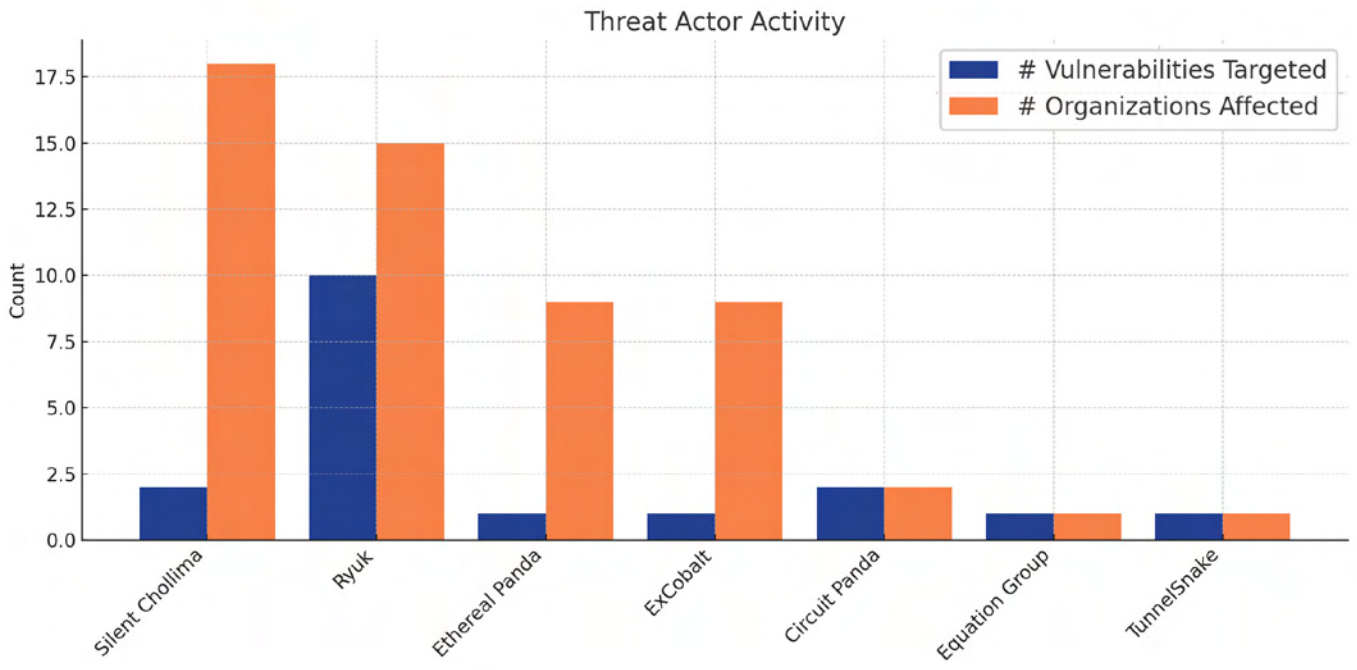
THREAT ACTOR ANALYSIS

OVERVIEW OF THREAT GROUPS KNOWN TO EXPLOIT THE CVES DETECTED

Research consistently shows that only a small percentage, typically 4% to 6%, of known CVEs are ever exploited in the wild. We can use rough numbers to make the point. The NIST National Vulnerability Database has more than 200,000 CVEs documented, while the CISA Known Exploited Vulnerabilities catalog has just 1,379 CVEs entries.

The takeaway is that any CVE known to be exploited in the wild is a major risk and should be prioritized for immediate remediation. CVEs with known exploitation activity should never be present in the external attack surface.

A small but significant portion of the CVEs uncovered by SixMap's research are known to be exploited by specific threat groups. While these groups have various motivations, origins, and tactics, any exploitation activity is a serious threat. Below is a summary of the threat groups known to exploit CVEs found among the 21 energy sector organizations in the sample group.



SILENT CHOLLIMA

AKA: APT45, ANDARIEL, ONYX SLEET, STONEFLY

Origin: North Korea

Overview:
A DPRK state-sponsored threat actor with activity dating back to at least 2007. Initially focused on espionage and destructive attacks, it's increasingly observed conducting financially motivated extortion campaigns.

Industries Targeted: Government, Defense, Energy, Aerospace, NGOs, Education, News Media

Regions Targeted: South Korea, United States, Japan, Europe

TTPs (MITRE ATT&CK):
Initial Access: Spearphishing (T1566), Malicious attachments, Social engineering
Execution: User execution (T1204), PowerShell (T1059.001)
Persistence: Registry run keys (T1547.001), Scheduled tasks (T1053.005)
Defense Evasion: Obfuscated files/scripts (T1027), Masquerading (T1036)
Credential Access: Credential dumping (T1003), Keylogging (T1056.001)
Collection: Email collection (T1114), Screen capture (T1113)
Command and Control: Custom C2 protocols (T1095), Web service (T1102)
Exfiltration: Exfiltration over C2 channel (T1041)

CVEs:
- CVE-2017-0199 (Microsoft Office/WordPad remote code execution)
- CVE-2018-4878 (Adobe Flash Player)
- CVE-2020-0601 (Windows CryptoAPI spoofing)
- CVE-2021-26411 (Internet Explorer RCE)

Victims:
- Korea Hydro & Nuclear Power
- Korea Atomic Energy Research Institute
- Various South Korean journalists and researchers
- U.S. think tanks and NGOs

EXCOBALT

AKA: COBALT GROUP, CARBANAK GROUP, GOLD KINGSWOOD

Origin: Russia

Overview:
ExCobalt is a financially motivated cybercriminal group from Russia, best known for targeting financial institutions and ATM networks. Their attacks often involve high-level social engineering, malware deployment, and direct theft from banks.

Industries Targeted: Financial Services (banks, payment systems), Hospitality (hotels), Retail

Regions Targeted: Europe (especially Eastern Europe), Russia/CIS, Asia, Latin America

TTPs (MITRE ATT&CK):
Initial Access: Spearphishing, Malicious attachments (T1566.001)
Execution: PowerShell, mshta, VBS scripts
Persistence: Scheduled tasks, Service creation
Credential Access: Credential dumping (T1003), Keylogging
Lateral Movement: RDP, PSExec
Command and Control: Custom C2, HTTP/S
Impact: Data theft, Wire fraud, ATM cashout1)

CVEs:
- CVE-2017-0199 (Microsoft Office)
- CVE-2018-8174 (Internet Explorer)
- CVE-2018-4878 (Adobe Flash Player)
- CVE-2019-0859 (Win32k)

Victims:
- Russian and Eastern European banks
- Financial institutions in Asia and Latin America

ETHEREAL PANDA

AKA: APT27, EMISSARY PANDA, LUCKYMOUSE, BRONZE UNION, TG-3390

Origin: China

Overview:
Ethereal Panda is a Chinese state-sponsored APT group involved in cyber-espionage, particularly targeting defense, technology, and government organizations. The group is known for large-scale, multi-year intelligence-gathering campaigns and data exfiltration.

Industries Targeted: Defense, Government, Energy, Aerospace, Technology

Regions Targeted: : United States, Europe, Southeast Asia, Middle East

TTPs (MITRE ATT&CK):
Initial Access: Spearphishing (T1566), Supply chain compromise (T1195), Web shells
Execution: Remote services (T1021), DLL side-loading (T1574.002)
Persistence: Web shells, Scheduled tasks (T1053)
Credential Access: Keylogging, Credential dumping (T1003)
Lateral Movement: Pass-the-Hash (T1075), RDP
Defense Evasion: Timestomping (T1070.006), Obfuscated files/scripts (T1027)
Command and Control: HTTP/S, Custom C2
Exfiltration: Exfiltration over web services (T1567.002)

CVEs:
- CVE-2017-11882 (Microsoft Office)
- CVE-2015-2545 (Microsoft Office)
- CVE-2014-4114 (Sandworm/Windows OLE)

Victims:
- U.S. defense contractors
- European government agencies
- Middle Eastern telecom providers

CIRCUIT PANDA

AKA: APT18, TG-0416, WEKBY

Origin: China

Overview:
Circuit Panda is a Chinese state-sponsored threat actor focused on cyber-espionage, particularly targeting the healthcare and pharmaceutical industries. Their activities include intellectual property theft, reconnaissance, and data exfiltration.

Industries Targeted: Healthcare and pharmaceuticals, Aerospace, Government, Manufacturing

Regions Targeted: United States, Europe, East Asia

TTPs (MITRE ATT&CK):
Initial Access: SQL injection (T1190), Phishing
Execution: Web shells, Remote code execution
Persistence: Web shells, Scheduled tasks
Defense Evasion: Obfuscated files/scripts
Credential Access: Credential dumping
Exfiltration: Exfiltration over C2 channels

CVEs:
- CVE-2014-6332 (Windows OLE)
- CVE-2015-4852 (Oracle WebLogic)
- CVE-2014-0160 (Heartbleed/OpenSSL)

Victims:
- U.S. health sector companies
- Aerospace firms

RYUK

NAMES: WIZARD SPIDER, GRIM SPIDER, UNC1878

Origin: Russia

Overview:
Ryuk is a notorious ransomware group. It is primarily financially motivated, targeting large organizations for extortion using malicious encryption malware. Ryuk became infamous for disrupting hospitals, municipalities, and major companies worldwide.

Industries Targeted: Healthcare, Government (cities/municipalities), Education, Manufacturing, Technology

Regions Targeted: United States, Europe (U.K., Germany, France, Spain), Middle East, Asia-Pacific

TTPs (MITRE ATT&CK):
Initial Access: Spearphishing, Exploitation of public-facing applications (T1190)
Execution: Custom rootkits, Living-off-the-land binaries
Persistence: Kernel/rootkit persistence (T1014)
Defense Evasion: Rootkit, Signed binaries, Process injection
Credential Access: Dumping credentials
Command and Control: Custom C2 protocols, Encrypted tunnels
Exfiltration: Exfiltration over C2

CVEs:
- CVE-2017-11882 (Microsoft Office)
- CVE-2019-0803 (Win32k Elevation of Privilege)
- CVE-2020-0688 (Microsoft Exchange)

Victims:
- Southeast Asian government ministries
- Middle Eastern diplomatic missions
- African governmental bodies

TUNNELSNAKE

AKA: UNC5221, MOSAICREGRESSOR

Origin: China

Overview:
TunnelSnake is a Chinese APT group, primarily known for its sophisticated attacks using custom rootkits (notably "Moriya") and targeting high-profile government and diplomatic organizations for espionage. The group's operations are marked by stealthy persistence and custom malware.

Industries Targeted: Government and diplomatic entities, Defense, NGOs

Regions Targeted: South and Southeast Asia, Middle East, Africa

TTPs (MITRE ATT&CK):
Initial Access: SQL injection (T1190), Phishing
Execution: Web shells, Remote code execution
Persistence: Web shells, Scheduled tasks
Defense Evasion: Obfuscated files/scripts
Credential Access: Credential dumping
Exfiltration: Exfiltration over C2 channels

CVEs:
- CVE-2014-6332 (Windows OLE)
- CVE-2015-4852 (Oracle WebLogic)
- CVE-2014-0160 (Heartbleed/OpenSSL)

Victims:
- U.S. health sector companies
- Aerospace firms

CONCLUSION

Cybersecurity teams at large American enterprises in the energy industry face major challenges. They must protect enormous attack surfaces, comprising thousands of hosts and assets, against the threat of highly sophisticated attackers who are targeting them. Every single exposure is a potential initial attack vector for the threat groups who seek to breach the network.

The 21 large energy industry organizations evaluated for this research project have massive digital estates that are invariably difficult to fully monitor, manage, and protect. It's important to highlight that security teams are not at fault for any unmanaged exposures or vulnerabilities.

In many cases, the limitations of traditional security tools are responsible. For example, legacy external attack surface management tools are designed to find unknown hosts but often fail to discover all of the shadow IT assets. Vulnerability management products are built to assess hosts and detect vulnerabilities but often scan only the top 1,000 or top 5,000 ports, leaving plenty of room for vulnerable services to exist in the shadows of non-standard ports.

SixMap brings several new innovations to the market that overcome the limitations of legacy security tooling. SixMap's computational mapping technology enables precise asset discovery across both the IPv4 and IPv6 address spaces, plus port inspection of all 65,535 ports for each asset. These capabilities result in more accurate and complete data on external assets, exposures, and vulnerabilities, so security teams can mitigate risks before an attack occurs.

Contact the SixMap team to gain access to complete and accurate exposure data.

CONTACT US

APPENDIX

Below is the full list of all 43 unique CVEs that are common to at least 45% (10 out of 21) of the energy sector organizations evaluated.

CV	SEVERITY	# OF COMPANIES	SERVICE	PORTS
CVE-2023-38408	Critical	16 (76.19%)	SSH	22, 70, 722, 2022, 2200, 2222, 2255, 5658, 7822, 21098, 41094
CVE-2024-38476	Critical	11 (52.38%)	HTTP	80, 81, 86, 90, 91, 92, 96, 443, 8000, 8001, 8002, 8007, 8080, 8081, 8088, 8089, 8090, 8091, 8092, 9090
CVE-2024-38475	Critical	11 (52.38%)	HTTP	80, 81, 86, 90, 91, 92, 96, 443, 8000, 8001, 8002, 8007, 8080, 8081, 8088, 8089, 8090, 8091, 8092, 9090
CVE-2024-38474	Critical	11 (52.38%)	HTTP	80, 81, 86, 90, 91, 92, 96, 443, 8000, 8001, 8002, 8007, 8080, 8081, 8088, 8089, 8090, 8091, 8092, 9090
CVE-2022-22721	Critical	10 (47.62%)	HTTP	80, 81, 86, 90, 91, 92, 443, 8080, 8092
CVE-2022-31813	Critical	10 (47.62%)	HTTP	80, 81, 86, 90, 91, 92, 96, 443, 8001, 8002, 8080, 8092, 9090
CVE-2022-22720	Critical	10 (47.62%)	HTTP	80, 81, 86, 90, 91, 92, 443, 8080, 8092
CVE-2022-28615	Critical	10 (47.62%)	HTTP	80, 81, 86, 90, 91, 92, 96, 443, 8001, 8002, 8080, 8092, 9090
CVE-2020-15778	High	16 (76.19%)	SSH	22, 70, 722, 2022, 2200, 2222, 5658, 7822, 21098, 41094
CVE-2021-41617	High	16 (76.19%)	SSH	22, 70, 722, 2022, 2200, 2222, 2255, 5658, 7822, 21098, 41094
CVE-2008-3844	High	16 (76.19%)	SSH	22, 70, 722, 2022, 2200, 2222, 2255, 5658, 7822, 21098, 41094
CVE-2023-51767	High	16 (76.19%)	SSH	22, 70, 722, 2022, 2200, 2222, 2255, 5658, 7822, 21098, 41094
CVE-2024-38472	High	11 (52.38%)	HTTP	80, 81, 86, 90, 91, 92, 96, 443, 8000, 8001, 8002, 8007, 8080, 8081, 8088, 8089, 8090, 8091, 8092, 9090

APPENDIX

CV	SEVERITY	# OF COMPANIES	SERVICE	PORTS
CVE-2024-38473	High	11 (52.38%)	HTTP	80, 81, 86, 90, 91, 92, 96, 443, 8000, 8001, 8002, 8007, 8080, 8081, 8088, 8089, 8090, 8091, 8092, 9090
CVE-2019-16905	High	11 (52.38%)	SSH	22, 70, 7822, 21098
CVE-2024-39573	High	11 (52.38%)	HTTP	80, 81, 86, 90, 91, 92, 96, 443, 8000, 8001, 8002, 8007, 8080, 8081, 8088, 8089, 8090, 8091, 8092, 9090
CVE-2024-40898	High	11 (52.38%)	HTTP	80, 81, 86, 90, 91, 92, 96, 443, 8000, 8001, 8002, 8007, 8080, 8081, 8088, 8089, 8090, 8091, 8092, 9090
CVE-2024-38477	High	11 (52.38%)	HTTP	80, 81, 86, 90, 91, 92, 96, 443, 8000, 8001, 8002, 8007, 8080, 8081, 8088, 8089, 8090, 8091, 8092, 9090
CVE-2025-30232	High	10 (47.62%)	SMTP	25, 26, 465, 587, 2525
CVE-2006-20001	High	10 (47.62%)	HTTP	80, 81, 86, 90, 91, 92, 96, 443, 8001, 8002, 8080, 8081, 8089, 8092, 9090
CVE-2022-30556	High	10 (47.62%)	HTTP	80, 81, 86, 90, 91, 92, 96, 443, 8001, 8002, 8080, 8092, 9090
CVE-2022-29404	High	10 (47.62%)	HTTP	80, 81, 86, 90, 91, 92, 96, 443, 8001, 8002, 8080, 8092, 9090
CVE-2022-22719	High	10 (47.62%)	HTTP	80, 81, 86, 90, 91, 92, 443, 8080, 8092
CVE-2023-38709	High	10 (47.62%)	HTTP	80, 81, 86, 90, 91, 92, 96, 443, 8000, 8001, 8002, 8080, 8081, 8088 8089, 8090, 8091, 8092, 9090
CVE-2023-31122	High	10 (47.62%)	HTTP	80, 81, 86, 90, 91, 92, 96, 443, 8000, 8001, 8002, 8080, 8081, 8088, 8089, 8090, 8091, 8092, 9090
CVE-2025-32728	Medium	16 (76.19%)	SSH	22, 70, 722, 2022, 2200, 2222, 2255, 5658, 7822, 21098, 41094

APPENDIX

CV	SEVERITY	# OF COMPANIES	SERVICE	PORTS
CVE-2023-48795	Medium	16 (76.19%)	SSH	22, 70, 722, 2022, 2200, 2222, 2255, 5658, 7822, 21098, 41094
CVE-2020-14145	Medium	16 (76.19%)	SSH	22, 70, 722, 2022, 2200, 2222, 2255, 5658, 7822, 21098, 41094
CVE-2007-2768	Medium	16 (76.19%)	SSH	22, 70, 722, 2022, 2200, 2222, 2255, 5658, 7822, 21098, 41094
CVE-2025-26465	Medium	16 (76.19%)	SSH	22, 70, 722, 2022, 2200, 2222, 2255, 5658, 7822, 21098, 41094
CVE-2016-20012	Medium	16 (76.19%)	SSH	22, 70, 722, 2022, 2200, 2222, 2255, 5658, 7822, 21098, 41094
CVE-2023-51385	Medium	16 (76.19%)	SSH	22, 70, 722, 2022, 2200, 2222, 2255, 5658, 7822, 21098, 41094
CVE-2019-6111	Medium	16 (76.19%)	SSH	22, 722, 2022, 2200, 2222, 5658, 41094
CVE-2018-15473	Medium	12 (57.14%)	SSH	22, 722, 2022, 2200, 2222, 5658, 41094
CVE-2018-20685	Medium	12 (57.14%)	SSH	22, 722, 2022, 2200, 2222, 5658, 41094
CVE-2017-15906	Medium	12 (57.14%)	SSH	22, 722, 2022, 2200, 2222, 5658, 41094
CVE-2018-15919	Medium	12 (57.14%)	SSH	22, 722, 2022, 2200, 2222, 5658, 41094
CVE-2019-6109	Medium	12 (57.14%)	SSH	22, 722, 2022, 2200, 2222, 5658, 41094
CVE-2019-6110	Medium	12 (57.14%)	SSH	22, 722, 2022, 2200, 2222, 5658, 41094
CVE-2022-37436	Medium	12 (57.14%)	HTTP	80, 81, 86, 90, 91, 92, 96, 443, 8001, 8002, 8080, 8081, 8089, 8092, 9090
CVE-2022-28330	Medium	10 (47.62%)	HTTP	80, 81, 86, 90, 91, 92, 96, 443, 8001, 8002, 8080, 8092, 9090
CVE-2022-28614	Medium	10 (47.62%)	HTTP	80, 81, 86, 90, 91, 92, 96, 443, 8001, 8002, 8080, 8092, 9090
CVE-2021-36368	Low	16 (76.19%)	SSH	22, 70, 722, 2022, 2200, 2222, 2255,

SIXMAP: TRUSTED BY SECURITY LEADERS AT THE WORLD'S LARGEST ORGANIZATIONS.

"Out of thousands of Internet-facing assets, SixMap was able to automatically pinpoint the most pressing vulnerabilities that required immediate action based on quantifying the risk by correlating the threat actors and exploitable vulnerabilities. We're glad they have partnered with AWS to deliver value to their customers."

Elwin Wong, CISO of Ross Stores

"One of the most powerful cybersecurity capabilities required to operate and defend computer networks … SixMap Computational Mapping provides public and private sector teams automation for network management and defense so that they can efficiently and effectively operate and defend IPv4-only, dual-stack, and IPv6-only networks."

United States Army, SBIR I Evaluation

SixMap provides the most accurate and complete external view of your organization—no input required, just the company name. Our preemptive exposure management platform interrogates all 65,535 ports as standard operating procedure—across IPv4 and IPv6—continuously hunting unknown assets, misconfigurations, and blindspots other tools miss. Built for security teams tired of tools that assume too much and miss even more, SixMap replaces guesswork with precision. So you can act faster, reduce exposure, and see what attackers see.

BOOK DEMO

SixMap, Inc.
6731 Columbia Gateway Dr Suite 100, Columbia, MD 21046

SIXMAP.IO