CYBLE

DATASHEET

Cyble Attack Surface Management

Identify and Secure All Areas That Could Be Targeted in Your Attack Surface

Introduction

Cyble's Attack Surface Management (ASM) enables organizations to gain visibility into their entire digital footprint and identify vulnerabilities before they become attack vectors. By continuously monitoring internet-exposed assets, Cyble ensures that security teams can detect and respond to potential risks across their attack surface, eliminating blind spots and protecting critical assets from unauthorized access.

Key Benefits

Eliminate Digital Risks

Identify and secure internet-exposed assets before they are exploited by malicious actors.

Eliminate Blind Spots

Use advanced AI models and Natural Language Processing (NLP) to analyze thousands of posts and uncover attack discussions.

Detect and Respond

Quickly determine the impact of data breaches or misconfigurations in your cloud storage environments.

Asset Intelligence

Gain comprehensive visibility and analysis of all your network's connected assets, both on-premises and in the cloud, to enhance security decision-making.

contact@cyble.com | www.cyble.com

Key Capabilities

- **Asset Discovery:** Cyble provides a centralized view of all assets, allowing security teams to streamline their management of potential attack points, conduct faster incident investigations, and improve vulnerability assessments.
- **Could Connectors:** Cyble's Cloud Connectors keep your organization's entire inventory seamlessly updated within the Cyble Attack Surface Management (ASM) platform. This ensures your security teams always have access to accurate, real-time data, eliminating the risk of working with incomplete or outdated information.
- **Vulnerability Management:** Full context on vulnerabilities within critical resources, enabling organizations to enhance their overall security posture by addressing and mitigating risks proactively.
- **Application Security Scanning:** Automated tools to scan web applications for vulnerabilities such as Cross-Site Scripting (XSS), SQL Injection, Command Injection, and insecure server configurations.
- **Code Repository Analysis:** Cyble leverages advanced scanning tools to analyze code repositories, identifying vulnerabilities and securing code practices.
- **SSL/TLS:** The SSL/TLS report delivers a comprehensive analysis of a web server's security, examining certificate details, supported protocols and ciphers, and identifying potential vulnerabilities. It also includes direct links to relevant security issues for easy reference and remediation.

How It Works

1. **Discover**
   Cyble continuously scans all internet-exposed assets, providing a comprehensive and centralized view of your attack surface, including on-premises and cloud assets.
2. **Analyze**
   AI-powered analysis tools scrutinize data for vulnerabilities, misconfigurations, and exposure points in your network, including code repositories and cloud storage environments.
3. **Detect**
   Cyble's system generates alerts for identified vulnerabilities, newly discovered ports, SSL expiry, domain expiry, and potential IP risks, allowing security teams to act swiftly.
4. **Mitigate**
   Actionable context and recommendations are provided with every alert, enabling organizations to prioritize security efforts and proactively defend against cyber threats.

See Cyble in action
https://cyble.com/request-demo/
www.cyble.com

Get in touch with us today
contact@cyble.com | +1 888 673 2067

About Cyble | The leader in External Cybersecurity
Cyble Inc. is a cybersecurity company specializing in dark web monitoring and threat intelligence services. Cyble leverages proprietary AI-based technology to help enterprises, federal bodies, and individuals stay ahead of cybercriminals. The company is known for its expertise in tracking cyber threats, data breaches, and other malicious activities.