CYBLE

DATASHEET

Attack Surface Management

Secure your digital assets through extensive attack surface management and actively protecting against threats.

Introduction

Cyble's Attack Surface Management (ASM) service provides organizations with a comprehensive, real-time solution to identify, monitor, and mitigate risks associated with their public-facing digital assets. By leveraging advanced threat intelligence and proprietary scanning technology, Cyble delivers proactive defense against emerging cyber threats.

Key Benefits

Continuously discovers and monitors
public-facing assets, including **shadow IT** components, ensuring complete visibility into an organization's external attack surface.

Offers holistic security exposure analysis
by identifying **misconfigurations, weak security settings, and unsecured services**, particularly across critical assets such as **email, DNS, SSL**, and exposed endpoints.

Automatically classifies security issues based on severity,
applying **risk-based scoring** to prioritize remediation efforts effectively.

With **continuous monitoring and automated risk assessment**, Cyble's ASM empowers organizations to **proactively manage security gaps, mitigate potential threats, and strengthen their overall cybersecurity posture.**

contact@cyble.com | www.cyble.com

Key Capabilities

1

Domains Discovery:

» Discovers the domains belonging to the customer organisations.

» Discovers domains with WHOIS protection enabled through connectors.

2

Subdomains Discovery:

» Subdomains discovery through different mechanisms

I. Open-Source Intelligence from passive sources

II. Certificate Transparency Logs

III. Passive DNS

IV. Active Internet Scanning through ODIN and pulling the digital certificates

V. Active keyword brute forcing strategies for the largest dictionary curated regularly from the most used patterns

3

IP Discovery:

» Through domains/subdomain resolutions.

4

IP Trace Discovery Path:

» IP discovery path creation through tracing mechanism to identify the source and ownership of it.

5

Digital Certificates Discovery:

» Active digital certificates discovery with daily updates to track the change of host ownership and any vulnerabilities related to it.

6

Open Ports Discovery:

» Active tracking of open ports for all IPs and Netblocks.

» Coverage up to 10k top ports.

7

DNS Records Discovery:

» All major types of DNS records discovery and any issues related to it.

8

Web Applications Discovery:

» Web applications exposed to the Internet are discovered using application tagging. The screenshot and favicon are captured to run through the further analysis process.

9

Shadow IT Discovery:

» Shadow IT assets are discovered through more extensive internet scanning. ODIN supercharges the discovery through reverse search for any assets belonging to the organisation that are exposed to the internet.

» ODIN scans 3 Billion IPs every 3 days across 500 ports for open ports and fingerprints their services and banner information.

10

Issue Catalog:

» Issue Catalog does non-intrusive application scanning by use of in-house & open-source templates. These templates cover various issues, like CVEs, misconfiguration, exposed panels, known vulnerabilities, default logins, subdomains takeovers, sensitive tokens, etc. Total templates of 9000+.

» Following Vulnerabilities are Supported

I. Web Application Vulnerabilities
II. SSL/TLS Vulnerabilities
III. DNS Vulnerabilities
IV. Open Port Vulnerabilities

11 **SSL\TLS Reports:**

» SSL\TLS reports cover checks of known vulnerabilities, such as Heartbleed, FREAK, outdated protocols enabled, and weak or insecure cipher suites

12 **DNS Security Issues:**

» DNS security issues such as SPF check, DMARC, DKIM, DNSSEC, Open Resolvers, and BIMI are covered.

13 **Domain & SSL Expiry:**

» Domain and SSL\TLS expiry are monitored and notified regularly.

14 **Network Services CVE:**

» Network vulnerabilities (CVEs) are captured from the detected open ports and their services. CVEs are further enriched with more information, such as exploitation and code publicly available information.

15 **Connectors:**

» Connectors allow you to connect with cloud providers, such as AWS, GCP, Azure, Digital Ocean, Akamai (Linode), and domain registries, such as GoDaddy, Namecheap, etc.

16 **On-demand scanning - OWASP Top 10:**

» On-demand OWASP Top 10 uses more comprehensive web application scanning. Web Application is crawled, and more active attacks like SQL Injection, XSS, SSRF, CSRF RCE, etc.

17 **On-demand scanning – Network:**

» On-demand Network scanning uses comprehensive scanning to find vulnerabilities in the open ports and their services.

18 **Vulnerability Intelligence:**

» Vision's Vulnerability Intelligence (VI) powers CVE association with discovered products

» VI currently covers over 10,000 vulnerabilities, including more than 1,200 critical vulnerability checks and over 2,000 high-severity ones.

» Cyble actively reviews all other templates and their associated data. Our internal Cyble Infosec team continuously develops new vulnerability templates to expand our coverage and ensures we stay ahead of emerging threats.

19 **Proof of Concept:**

» ASM provides detailed vulnerability descriptions, along with Proof of Concept (POC) demonstrations, which allow customers to replicate and understand each vulnerability better.

» With Cyble AI, tailored impact assessments, recommendations, and references are generated for every vulnerability, giving customers comprehensive insights into the issue. This combination of information helps customers understand the overall risk profile and take appropriate mitigation steps. All of this is reviewed by our internal InfoSec team to ensure accuracy.

20 **Risk Scoring :**

» Our risk scoring methodology is comprehensive, covering several critical parameters such as the severity of vulnerabilities, exploitability, potential business impact, and the presence of compensating controls. These factors are weighted and normalized to generate an overall risk score, providing customers with a clear, actionable understanding of their security posture. The risk scores allow organizations to prioritize remediation efforts by focusing on the most critical vulnerabilities.

How It Works

1 **Discovery:**
ASM begins by identifying all internet-facing assets, including those that may be unknown or unmanaged. This comprehensive asset discovery is achieved through continuous scanning of networks to ensure that no digital assets are overlooked.

2 **Assessment:**
Once assets are identified, the platform evaluates the risks and vulnerabilities associated with these assets. This includes analyzing configurations, detecting misconfigurations, and identifying weaknesses that could be exploited by attackers.

3 **Mitigation:**
After assessing the vulnerabilities, Cyble's ASM provides actionable recommendations to address identified vulnerabilities, assisting organizations in strengthening their security posture. This may involve patching software, reconfiguring settings, or decommissioning unused assets.

4 **Continuous Monitoring:**
The platform offers real-time surveillance of digital assets, promptly detecting vulnerabilities and potential attack vectors, thereby enabling swift remediation. This continuous monitoring ensures that organizations maintain an up-to-date understanding of their attack surface and can respond quickly to any changes or emerging threats.

Scan the QR code to get a quick personalized demo of our AI-powered Threat Intelligence platform in action!

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.