praetorian

Attack Surface Management

A Free Enablement Technology for Effective Continuous Threat Exposure Management

Introduction

In the ever-evolving landscape of cybersecurity, organizations are increasingly focusing on their attack surfaces to identify and mitigate potential risks. However, the current state of Attack Surface Management (ASM) is often nothing more than inactionable asset discovery. After mapping an organization's attack surface, many are left wondering, "So what?" and "Now what?" At Praetorian, we challenge this norm by offering a free version of our Chariot platform, including its powerful ASM scanning capabilities. Our goal is to provide organizations with the essential tools needed to stay ahead of potential attacks, emphasizing that the real value lies in identifying and mitigating material risks as part of a comprehensive Continuous Threat Exposure Management (CTEM) program.

The Problem with Current Practices

Today's ASM solutions frequently stop at asset discovery, leaving organizations with a comprehensive map of their attack surface but no actionable insights. This "so what" and "now what" dilemma results in organizations struggling to prioritize and address their most critical risks. The reliance on external bug bounty programs and vulnerability researchers often leads to significant costs and a reactive security posture, where organizations respond to immediate threats rather than managing their overall risk landscape proactively.

This approach inadvertently empowers attackers. By paying for vulnerabilities, organizations may foster an environment where attackers are incentivized to find and exploit weaknesses rather than focusing on systemic improvements in security posture.

Praetorian's Vision: Free Attack Surface Management

At Praetorian, we believe that attack surface management should be a foundational capability available to all organizations without cost. ASM is a crucial enablement technology that provides visibility into potential attack vectors, allowing organizations to understand their exposure and take proactive measures. By offering our ASM module for free within the Chariot platform, we aim to shift the focus from reactive vulnerability discovery to proactive risk management.

Key Features of Chariot's Attack Surface Management Module

Our Chariot platform includes a comprehensive attack surface module designed to provide deep insights into an organization's assets and attack surface. Asset identification and attack surface mapping include both outside-in attack enumeration and inside-out system of record integrations.

Current integrations supported under freemium include:

aws

CLOUDFLARE

NS1.

GitHub

GitLab

ADDITIONAL FEATURES INCLUDE

Exposed Secrets in Code
Automatically identifying secrets that have been inadvertently exposed in public or private repositories.

Repository Status Changes
Monitoring changes from private to public repository status to ensure sensitive information is not unintentionally exposed.

New Public Repositories
Detecting the addition of new public repositories to manage and mitigate potential risks.

Vulnerabilities in GitHub Self-Hosted Runners
Identifying and addressing vulnerabilities in self-hosted runners used for CI/CD pipelines.

These features, along with many others, are available at no cost, empowering organizations to maintain robust security postures without the financial burden typically associated with vulnerability discovery.

Shifting the Focus to Material Risks

While attack surface management provides essential visibility, the true value lies in the actionable insights derived from this information. In the context of a CTEM program, the goal is not merely to identify potential vulnerabilities but to prioritize and address the most significant risks. This involves:

Vulnerability Prioritization

Using ASM data to prioritize vulnerabilities based on their potential impact on the organization. This ensures that resources are focused on the most critical issues.

Continuous Monitoring

Implementing continuous monitoring to detect and respond to new threats as they emerge, maintaining an adaptive and resilient security posture.

Threat Intelligence Integration

Leveraging threat intelligence to contextualize vulnerabilities within the broader threat landscape, enhancing the ability to anticipate and mitigate attacks.

Conclusion

Attack surface management should be viewed as an integral part of a comprehensive cybersecurity strategy, not a standalone service that incurs additional costs. By offering our ASM capabilities for free through the Chariot platform, Praetorian aims to democratize access to essential security tools, enabling organizations to focus on identifying and mitigating material risks. This proactive approach to vulnerability management and continuous threat exposure management represents the future of cybersecurity, where the emphasis is on strategic risk reduction rather than reactive vulnerability patching.

Learn more about the risks associated with GitHub and how Praetorian is working to mitigate them through our Chariot platform. Empower your organization with the tools needed to stay ahead of potential attacks and shift the focus from vulnerability discovery to proactive risk management.