White Paper for Attack Surface Management

Presented by

ZERON

World's 1st Autonomous
Cyber Risk Posture Management Platform

White Paper for Attack Surface Management by ZERON

This white paper introduces ZERON's External Attack Surface Management (EASM) solution, a state-of-the-art tool designed to tackle the challenges of securing modern internet-facing assets. Providing extensive threat detection and analysis, EASM automates asset discovery, offers comprehensive domain-wise monitoring, ensures real-time visibility, and integrates seamlessly with existing security frameworks. With capabilities such as dynamic scanning, risk prioritization, and detailed vulnerability insights, the EASM solution significantly reduces the time, effort, and potential errors associated with traditional external risk management processes.

Introduction

In today's digital landscape, organizations face an ever-increasing array of cyber threats. These threats exploit vulnerabilities in the external attack surface, comprising all the internet-facing assets that an organization possesses. External Attack Surface Management (EASM) is a crucial practice for identifying, monitoring, and mitigating these vulnerabilities to ensure robust cybersecurity defense.

Problem Statement

Organizations often struggle with maintaining visibility and control over their external attack surface due to its dynamic and expansive nature. Traditional security measures are insufficient to manage the complexity and scale of internet-facing assets, leaving organizations exposed to cyber threats. The inability to accurately identify and prioritize vulnerabilities results in inefficient resource allocation and increased risk of data breaches.

Solution Overview

External Attack Surface Management (EASM) provides a proactive and comprehensive approach to identifying, monitoring, and securing all internet-facing assets. By leveraging advanced technologies and methodologies, EASM enables organizations to maintain continuous visibility of their external attack surface, prioritize vulnerabilities based on risk, and implement effective mitigation strategies.

Technical Details

1. Automated Scanning and Visualization

- Comprehensive Visualization: EASM presents a holistic view of the organization's entire attack surface, allowing for thorough assessment and understanding of potential vulnerabilities.
- Dynamic Scanning: Conducts continuous and dynamic scanning across multiple domains, customizable to the organization’s needs.
- Tailored Scan Intervals: Enables ongoing surveillance of publicly available resources by setting specific scan intervals.
- Asset Tracking and Classification: Automatically tracks and classifies publicly available assets, providing a detailed profile of vulnerabilities associated with each asset.

2. Denoised Attack Surface Management

- Refined Approach: Utilizes advanced algorithms to reduce irrelevant findings, ensuring security teams focus on genuine threats and vulnerabilities.
- Enhanced Efficiency: By minimizing noise, EASM enhances the efficiency and response times of security teams.

3. Exposed Panels and WAF Protection Insights

- Thorough Detection: Identifies digital assets across the internet, including cloud services, web applications, and connected devices.
- Security Posture Strengthening: Provides visibility into exposed panels, default credentials, and login points, crucial for enhancing security measures.
- Comprehensive Visibility: Detects and provides detailed insights into WAF-protected assets, enabling a complete understanding of protected assets and vulnerabilities.
- Proactive Mitigation: Helps security teams develop proactive strategies to mitigate potential threats.

4. Exploitability and Cloud Exposures

- Vulnerability Assessment: Assesses vulnerabilities based on their exploitability score, ensuring resources are allocated effectively to mitigate high-risk threats.
- Visibility into Cloud Data: Provides insights into publicly accessible data hosted in the organization’s cloud, highlighting potential exposure of confidential and sensitive information.

5. Attack Surface Monitoring and Threat Classification

- Vulnerability Identification: Identifies potential vulnerabilities and weak points within the organization's domain infrastructure.
- Risk Probability Assessments: Offers risk probability assessments and prioritization for every potential vulnerable asset.
- IP and Subdomain Insights: Provides a comprehensive list of linked IP addresses and subdomains, with real-time categorization and detailed insights into critical vulnerabilities.
- Port Diagnostics: Enhances security by providing port diagnostics for IP addresses, fortifying potential entry points.
- Automated Minimization: Employs automated mechanisms to reduce the organization's attack surface and provides recommendations for mitigating exposure to threats.
- Threat Aggregation: Aggregates threats related to specific attack surface assets, enabling security teams to focus on areas with concentrated risk.

Benefits and Advantages

- Continuous Visibility: Ensures real-time, continuous visibility of the organization’s external attack surface.
- Efficient Resource Allocation: Enables effective prioritization of vulnerabilities based on risk, optimizing resource allocation.
- Enhanced Security Posture: Provides comprehensive insights and proactive measures to strengthen the organization’s security posture.
- Reduced Risk of Data Breaches: Minimizes exposure to cyber threats, significantly reducing the risk of data breaches.
- Improved Response Times: Streamlines the identification and mitigation of genuine threats, enhancing response times and efficiency.

Conclusion

External Attack Surface Management is a critical component of modern cybersecurity strategies. By providing comprehensive visibility, proactive monitoring, and effective mitigation of vulnerabilities, EASM enables organizations to protect their internet-facing assets and maintain a robust security posture. Implementing EASM ensures that organizations can stay ahead of cyber threats, allocate resources efficiently, and minimize the risk of data breaches in an increasingly complex digital environment.