WHITE PAPER

Difference Between Effective Attack Surface Management (EASM) & Cyber Attack Surface Management (CAASM)

LUCIDUM

NOW PART OF cyderes

Introduction

As a newly appointed Chief Information Security Officer (CISO), you have an important role to play in ensuring the security of your organization. The first 90 days in this role is critical to establishing a solid foundation for your cybersecurity strategy. One of the key components to consider is Cyber Asset Attack Surface Management (CAASM).

CAASM is a proactive approach to identifying and mitigating vulnerabilities in an organization's technology infrastructure. By implementing CAASM, you can reduce the risk of a successful cyber attack, comply with regulations, and gain visibility into your organization's attack surface. In this guide, we will outline the steps you can take in the first 90 days to be successful with CAASM.

Effective Attack Surface Management (EASM)

EASM is the process of identifying and managing the attack surface of an organization. This includes identifying all assets that make up the attack surface, including servers, network devices, cloud resources, mobile devices, and IoT devices. The goal of EASM is to understand the attack surface, identify vulnerabilities, and prioritize them based on their criticality. After vulnerabilities have been identified, EASM implements mitigation measures to address the most critical vulnerabilities. This might include patching, configuring security settings, or implementing additional security controls. EASM is a continuous process and requires ongoing monitoring and support to ensure that new vulnerabilities are identified and addressed in a timely manner.

Cyber Asset Attack Management (CAASM)

CAASM is a subset of EASM that focuses on the management of cyber assets, including servers, network devices, cloud resources, mobile devices, and Iot devices. The goal of CAASM is to identify, inventory, and understand the cyber assets that make up an organization's attack surface and to identify and prioritize vulnerabilities in those assets.

CAASM also implements mitigation measures to address the most critical vulnerabilities and performs ongoing monitoring and support to ensure that new vulnerabilities are identified and addressed in a timely manner. In addition, CAASM prioritizes ongoing vulnerability remediation, vulnerability management, and vulnerability intelligence.

Key Differences

While EASM and CAASM are both important for managing an organization's attack surface, there are key differences between the two:

01.

Scope: EASM is broader in scope, focusing on all assets that make up an organization's attack surface, while CAASM is focused specifically on the management of cyber assets.

02.

Focus: EASM focuses on understanding the attack surface and identifying and mitigating vulnerabilities, while CAASM also prioritizes vulnerability remediation, vulnerability management,

03.

Compliance: EASM is typically used to comply with regulations and industry standards, while CAASM is used to comply with specific regulations that apply to the management

LUCIDUM

Conclusion

In conclusion, Effective Attack Surface Management (EASM) and Cyber Asset Attack Surface Management (CAASM) are important components of an organization's cybersecurity strategy. EASM is a broad-based approach that focuses on understanding and managing the entire attack surface, while CAASM is focused specifically on the management of cyber assets.

Both are important, and organizations should consider using both EASM and CAASM as part of a comprehensive approach to managing their attack surface. Understanding the differences between these two concepts and incorporating them in a strategic and holistic way can help organizations to proactively reduce the risk of a successful cyber attack, comply with regulations, and gain visibility into their organization's attack surface.

About Lucidum

Lucidum was built by cybersecurity experts on a mission to gain full visibility into their tech ecosystem. We take pride in our innovative platform, and we're thrilled each time we offer our customers the ability to see and understand what was formerly lurking just off the radar.

We put everything in your sights, giving you the power to understand what it is and what it's doing. Understand the lay of your tech landscape, lock onto threats, and keep your perimeter secure – all empowering you to defend and dominate your space in an increasingly threatening world.

Learn more at www.lucidum.io

LUCIDUM