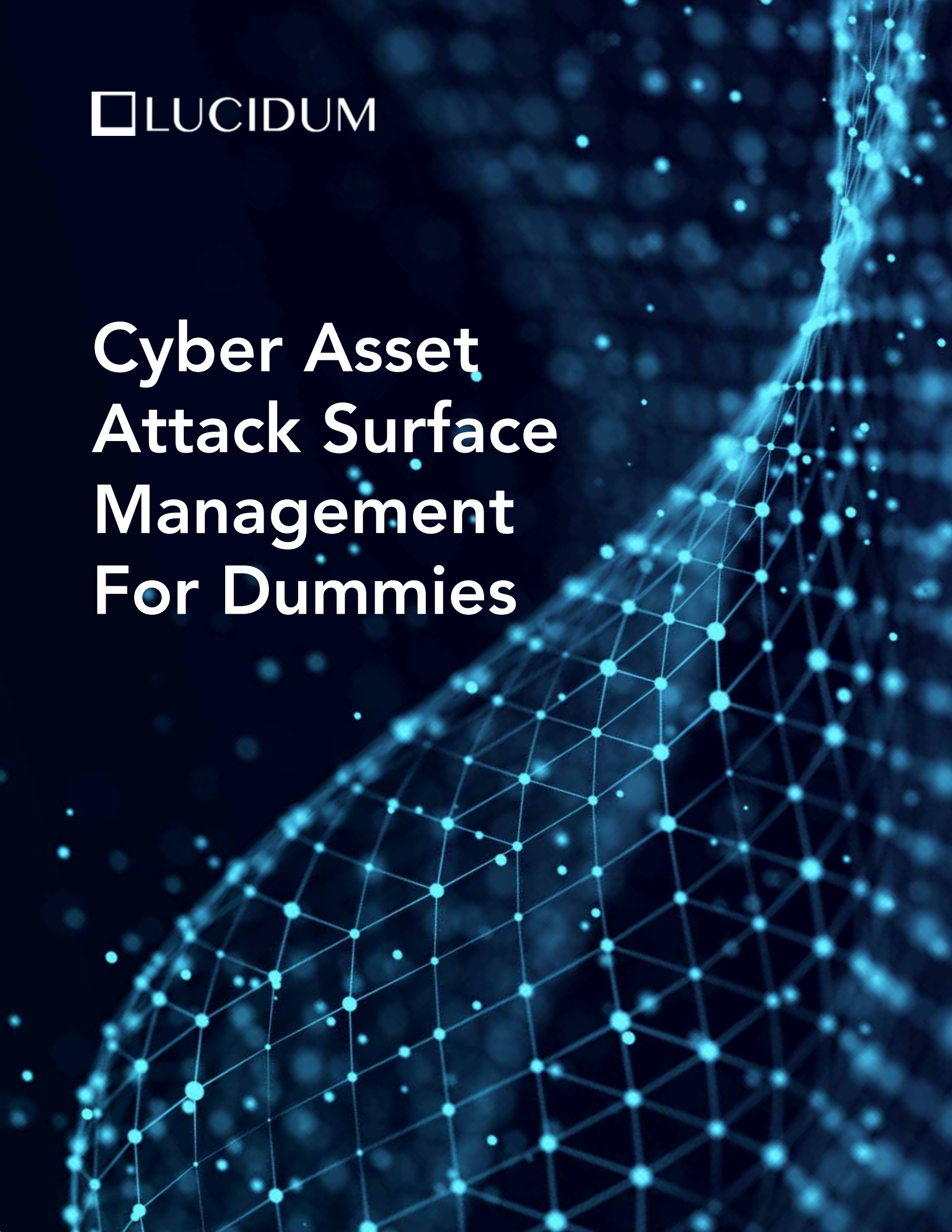
LUCIDUM

Cyber Asset Attack Surface Management For Dummies



INTRODUCTION

Cybersecurity is becoming more important than ever, as businesses and individuals become increasingly reliant on technology to store, process and transmit information. However, with the constant evolution of technology and the increasing number of cyber threats, it can be difficult for organizations to keep their technology infrastructure secure.

Cyber Asset Attack Surface Management (CAASM) is a proactive approach to identifying and mitigating vulnerabilities in an organization's technology infrastructure. It is a critical component of an organization's cybersecurity strategy and can help to reduce the risk of a successful cyber attack.

What is Cyber Asset Attack Surface Management (CAASM)?

CAASM is the process of identifying and managing all assets that make up an organization's attack surface, including servers, network devices, cloud resources, mobile devices, and IoT devices. By identifying these assets and analyzing them for vulnerabilities, organizations can take steps to mitigate the risk of a successful cyber attack.

CAASM involves a number of different steps, including:

- Identifying all assets that make up the organization's attack surface
- Analyzing the assets to identify vulnerabilities that could be exploited by an attacker
- Prioritizing vulnerabilities based on their criticality
- Implementing mitigation measures to address the most critical vulnerabilities
- Ongoing monitoring and support to ensure that new vulnerabilities are identified and addressed in a timely manner

Why is CAASM important?

CAASM is important for a number of reasons, including:

01 **Proactive Risk Management:** By identifying and mitigating vulnerabilities in an organization's technology infrastructure, CAASM helps to reduce the risk of a successful cyber attack before it happens. specifically on the management of cyber assets.

02 **Identify and Prioritize Vulnerabilities:** iCAASM helps organizations to identify all assets that make up their attack surface, including servers, network devices, cloud resources, mobile devices, and IoT devices. By analyzing these assets for vulnerabilities, organizations can prioritize the vulnerabilities to address first, by their criticality.

03 **Keep Up-to-Date with Current Best Practices:** Cybersecurity is constantly evolving, and new threats and vulnerabilities are identified all the time. By providing ongoing monitoring and support, organizations can ensure that they are aware of these new threats and are taking the necessary steps to mitigate them.

04 **Meet Compliance Requirements:** Many organizations are subject to compliance requirements, such as those imposed by governments, industry standards, and regulations. CAASM can help organizations comply with these regulations by providing a comprehensive service to manage their attack surface.

05 **Increase Efficiency:** By identifying and mitigating vulnerabilities in an organization's technology infrastructure, CAASM helps prevent costly security breaches. This prevention can have a major impact on an organization's bottom line and increase efficiency by reducing downtime caused by security breaches.

06 **Differentiate from Competitors:**
Offering CAASM as a service can help organizations differentiate themselves from their competitors and attract potential customers who are looking for a comprehensive cybersecurity service

07 **Provide Peace of Mind:**
By managing their attack surface, organizations can give their employees and customers peace of mind and enable them to focus on their core operations. This is an essential aspect of an organization's cybersecurity strategy.

Implementing CAASM

Implementing CAASM involves several key steps, including:

Asset Identification

The first step in implementing CAASM is to identify all assets that make up an organization's attack surface. This includes servers, network devices, cloud resources, mobile devices, and IoT devices.

Vulnerability Analysis

After assets have been identified, they should be analyzed for vulnerabilities that could be exploited by an attacker. This can be done manually with vulnerability scans, penetration testing, and other security assessments, or it can be done using automated tools

Prioritization

After vulnerabilities have been identified, they should be prioritized by criticality. This can be done by assessing the potential impact of a successful attack and the likelihood of it happening. Critical vulnerabilities should be addressed first.

Mitigation

After prioritizing vulnerabilities, mitigation measures should be implemented to address the most critical vulnerabilities. Mitigation can include applying software patches and configuration changes, implementing firewalls and intrusion detection systems, and implementing security policies and procedures.

Ongoing Monitoring & Support

AASM is not a one-time process, it is an ongoing effort.

CONCLUSION

In conclusion, Cyber Asset Attack Surface Management (CAASM) is an essential service for organizations to protect and manage their technology infrastructure from cyber threats. By identifying and mitigating vulnerabilities in an organization's attack surface, CAASM helps organizations to proactively reduce the risk of a successful cyber attack, comply with regulations, increase efficiency, and provide peace of mind. Implementing CAASM requires regular monitoring and support.

By implementing CAASM, organizations can be proactive in protecting their technology infrastructure and increasing their cybersecurity posture. Organizations should consider incorporating CAASM as a core component of their cybersecurity strategy and work with a reputable managed security service provider (MSSP) who can provide this service and ensure that their infrastructure is always up-to-date with the latest best practices and guidelines.

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**