WHITEPAPER

7 REASONS Why MSSPs Need Cyber-Asset Attack Surface Management For Their Customers

LUCIDUM

7 REASONS

WHY MSSPs NEED YBER-ASSET ATTACK SURFACE MANAGEMENT FOR THEIR CUSTOMERS

Managed Security Service Providers (MSSPs) play a critical role in helping organizations protect their technology infrastructure from cyber threats. Cyber Asset Attack Surface Management (CAASM) is an essential service that MSSPs can provide to their clients that can assist in detecting, managing, and reducing the risk of a cyber attack.

By identifying and mitigating vulnerabilities in an organization's attack surface, MSSPs can help prevent costly security breaches, comply with regulations and increase their own profit margins. This whitepaper will outline the 7 key reasons how MSSPs would benefit from CAASM. It will also show how MSSPs can provide a comprehensive service to manage their clients' attack surface, providing the necessary protection to their clients and giving them the ability to meet compliance requirements, increase their profit margins, and increase peace of mind.

01.

Proactive Risk Management: Cyber Asset Attack Surface Management (CAASM) is a proactive approach to identifying and mitigating vulnerabilities in an organization's technology infrastructure. By providing CAASM as a service, MSSPs can help their clientsreduce their risk of a successful cyber attack before it happens.

02.

Identify and Prioritize Vulnerabilities: ASM helps MSSPs identify all assets that make up the client's attack surface, including servers, network devices, cloud resources, mobile devices, and IoT devices. MSSPs can then analyze these assets to identify vulnerabilities that could be exploited by an attacker. By prioritizing vulnerabilities, MSSPs can ensure that the most critical ones are addressed first.

LUCIDUM

03.

Keep Up-to-Date with Current Best Practices: Cybersecurity is a constantly evolving field, and new threats and vulnerabilities are being identified all the time. By providing ongoing monitoring and support, MSSPs can ensure that their clients 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 the government, industry standards and regulations. MSSPs can help their clients to comply with these regulations by providing a comprehensive service to manage their attack surface.

05.

Increase Profit Margins: MSSPs can increase their profit margins by providing ASM as a service. By identifying and mitigating vulnerabilities in their clients' technology Infrastructure, MSSPs can help prevent costly security breaches, which can have a major impact on an organization's bottom line.

06.

Differentiate from Competitors: Offering CAASM as a service can help MSSPs differentiate themselves from their ompetitors, and attract potential customers who are looking for a comprehensive cybersecurity service.

07.

Provide Peace of Mind: By managing their clients' attack surface, MSSPs can give their clients peace of mind and enable them to focus on their core operations, this is an essential aspect of an organization's cybersecurity strategy.

With the increase of ever-evolving cyber threats, it is becoming more and more important for MSSPs to adopt CAASM as a core component of their cybersecurity strategy.

LUCIDUM

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