WHITEPAPER

YOUR FIRST 90 DAYS AS A CISO

Be Successful With Cyber -Asset Attack Surface Management

LUCIDUM

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.

01.

Assess your current cybersecurity posture: The first step in implementing CAASM is to assess your current cybersecurity posture. This includes identifying all assets that make up your organization's attack surface, including servers, network devices, cloud resources, mobile devices, and IoT devices. By understanding your current posture, you can identify vulnerabilities and prioritize them based on their.

02.

Implement mitigation measures: 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.

03.

Establish ongoing monitoring and support: CAASM is not a one-time process but an ongoing effort, so it's important to establish ongoing monitoring and support to ensure that new vulnerabilities are identified and addressed in a timely manner. This may include implementing automated scanning tools, regular penetration testing and incident response procedures.

LUCIDUM

04.

Communicate with stakeholders: Communication is key when implementing new security measures, including CAASM. Make sure to keep all stakeholders informed about the new measures being put in place, and the rationale behind them. This can help to build support for your cybersecurity strategy, and ensure that everyone is aware of their responsibilities.hensive service to manage their attack surface.

05.

Continuously improve: Your first 90 days as a CISO is only the beginning of your journey, security threats and organization needs change constantly, so it's important to continuously eview and improve your CAASM program. Continuously review, and evolve the program by gathering feedback from stakeholders and teams, and by keeping up to date with industry best practices.

Conclusion

Implementing Cyber Asset Attack Surface Management (CAASM) in the first 90 days as a CISO is a critical step in establishing a solid foundation for your cybersecurity strategy. By proactively identifying and mitigating vulnerabilities in your organization's technology infrastructure, you can reduce the risk of a successful cyber attack, comply with regulations, and gain visibility into your organization's attack surface. Through continuously monitoring and improvement, you can ensure that your CAASM program keeps up with the ever-evolving cybersecurity landscape.

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.

LUCIDUM