Validating Attack Surface Management ASsuMptions

May 23, 2022

Director, Community Ecosystem Engagement - Cybersecurity

Michael is a world-leading IT industry analyst. He has led North American and global initiatives focused on developing insights and strategies that connect technology solutions with business needs, combining data, knowledge, analysis and advanced content delivery to define options for IT and buy-side businesses.

Submitted by Michael O'Neil on 23, May 2022

Validating Attack Surface Management ASsuMptions

After publishing the landmark *Automating Defense: Implementing Continuous Discover and Validation* Horizon Report, Stratascale convened an exclusive panel of client CISOs to discuss attack surface management (ASM) and automated discovery and validation.

Stratascale VP for the Office of the CISO Michael Wilcox, Director of Security Operations Advisory Services Ryan Benson, Senior Technical Advisor Joseph Karpenko, and Lead Cybersecurity Analyst Michael O'Neil kicked off the session with our guest CISOs by examining four assumptions that underlie the research:

- Attack surface isn't something that everybody grasps—it can be difficult to fully define and manage.
- Not everyone is doing continuous validation; there is still extensive use of periodic pen tests.
- Digital transformation has moved so fast that security has been unable to fully keep up.
- There is tension between the increasing volume, velocity, and variety of data and a shortage of talent to evaluate and act on that data, creating a need to develop context that will support action.

Discussion on these points helped shape the deeper roundtable discussion of ways to establish ASM within F1000 businesses. Some of the highlights included:

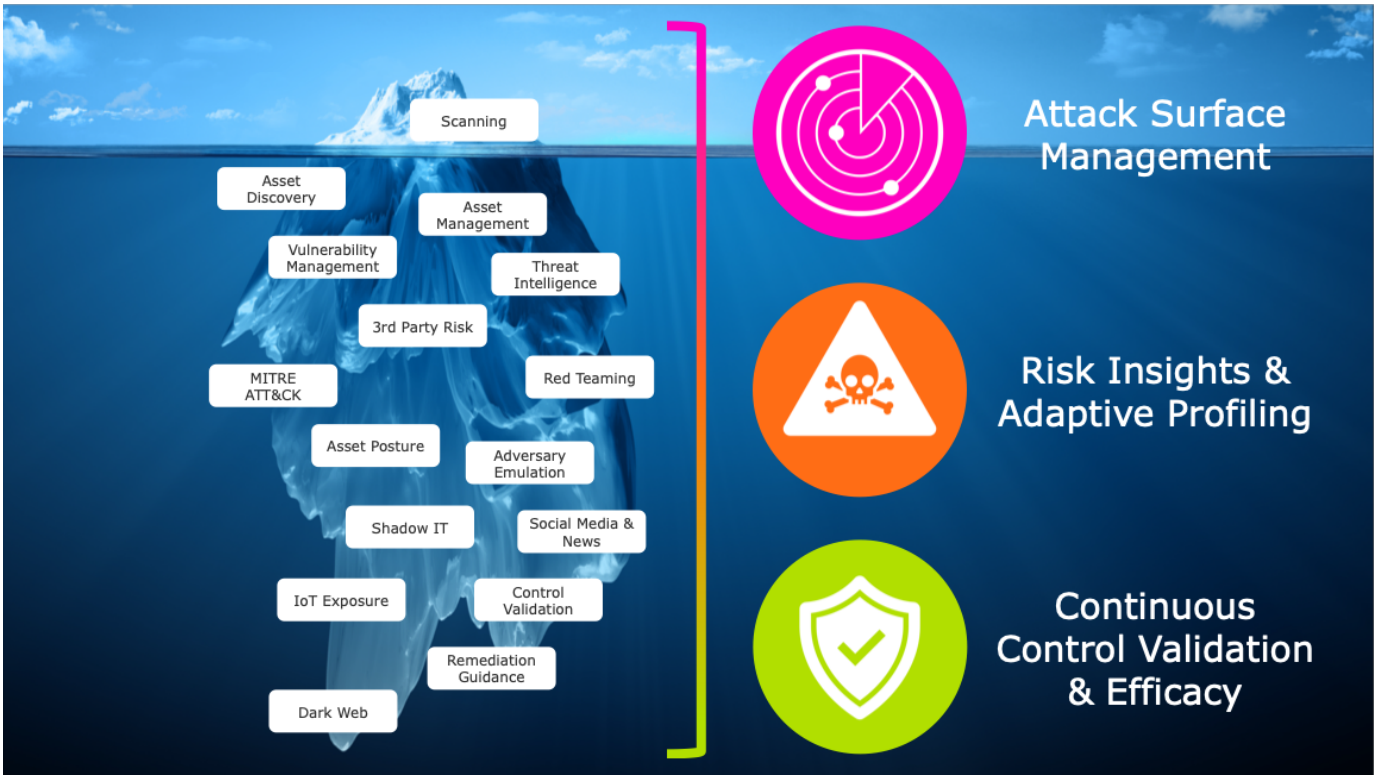
- **General agreement that there are corporate-level gaps in grasping what the attack surface actually represents.** One CISO explained this by noting that "within *security*, we have a pretty good handle [on the corporate attack surface], but there are educational requirements in other areas of the business." Another highlighted the challenges posed by a continuously-changing landscape: "everyone's trying to automate, trying to economize…[but] how do we package this, how do we communicate it to leadership?" A third chimed in on this theme, asking, "Will management then fund what is appropriately understood?"
- **Continuous validation is desirable, but not a common attribute of ASM strategies.** "We definitely aren't doing continuous validation," one participant admitted. Another expanded on the need to couple automation with human actors: "not everyone is doing this – breach sim with vulnerability scanning – but periodic red team exercise for me is critical. They are 'spot in time,' but

there’s no substitute for a live, thinking, human adversary. They’re going to find things that the tools will never find.” Further discussion in this area helped elucidate the value of continuous testing – “if you want your money’s worth, you don’t want to be testing against last week’s exploits” – and a more general move towards risk-based scoring, which led one CISO to ask aloud, “Do even mature organizations have blind spots?”

- **Digital transformation initiatives are not currently overwhelming ASM capabilities.** CISOs participating in the roundtable discussion were not persuaded that digital transformation is exacerbating existing gaps between business requirements and security capabilities. This may be an issue of maturity within both the security operation and the business as a whole. One CISO said, “we see more digital transformation *within* security than in other parts of the business;” another reported that “here, the macro environment isn’t changing all that fast.”
- **The problem isn’t really the volume of data – it’s the availability of people.** The final assumption sparked an extended discussion about staffing challenges. One CISO noted that their organization “has been consistently 30% under [target] headcount for a year and a half.” Later, a participant lamented the disconnect between norms in cybersecurity and other parts of the business: “we’ve had fairly high turnover – 10-15% a year,” which was not seen as uncommon in the cybersecurity ranks, but which raises the hackles of HR departments that are accustomed to lower turnover rates in other parts of the business.

The examination of core assumptions provided the roundtable with a strong basis for a deeper dive into investment drivers and actions addressing ASM and automation, tracking through the “iceberg” diagram that was used to surface specific ASM considerations. The balance of the roundtable session dealt with a number of related issues – success metrics, budgets, and ways of integrating security into business processes – that branch through and beyond ASM, and which have already provided grist for further discussion.

Thinking back on the roundtable, though, the examination of underlying assumptions stands out as an essential first step in building insight for everyone involved in the session. In both best practice analysis and in cybersecurity operations, a well-defined foundation is a critical element of success.



How Stratascale can help: *Stratascale's ATLAS service is designed to address the problem of external cyber risk through continuous attack mapping and validation. By surveying and verifying the overall attack surface of the organization, ATLAS helps large companies overcome shortages of people, processes, or tools, and enables them to integrate critical attack surface data into their existing SOC and/or MSSP/MDR solutions. This allows companies to understand and prepare for the most probable cyberattacks with the right security controls, detections, and response actions.*

If you're ready to learn more about how ATLAS can help protect your organization's assets, reach out to ATLAS@stratascale.com.