SANS

Analyst Program

Survey

Building a Resilient Offensive Security Strategy

Written by **Matt Bromiley**

November 2023

hackerone

Executive Summary

An offensive security strategy is a proactive and essential approach to safeguarding an organization's digital assets in an increasingly hostile cyber landscape. Adversaries hone their skills daily, and the threat landscape is rife with ever-changing threats. An offensive mindset mimics adversaries' tactics to identify vulnerabilities and weaknesses before they can be exploited.

Offensive strategies also help enhance an overall security posture. By actively seeking out vulnerabilities through activities like vulnerability scanning and penetration testing, security teams can address gaps before they are exploited. A resilient and responsive cybersecurity posture is established through continuous assessment of systems.

Attack surface management (ASM), is integral to a broad offensive security strategy. With proactive identification and classification of an external attack surface, a security team is empowered with actionable intelligence. ASM enables teams to focus their offensive security efforts on pinpointing and exploiting weaknesses before adversaries can.

In this survey, we set out to understand how organizations integrate ASM within a comprehensive offensive security framework and whether that knowledge impacts risks, mitigations, and security priorities. Often, the ideal security state is easier said than done. Security implementations can take months or years, with process changes taking just as long (or longer!). As we walk through this survey, we encourage you to compare your offensive security strategy and the use of ASM against what our respondents reported.

In particular:

- Does your organization have concern for unknown risks, and does this impact your offensive security strategy?
- How do the findings from your offensive actions impact risk exposure and mitigation?
- How does ASM fit within your broader offensive security strategy?

For some, considering offensive security actions can be a new endeavor. However, for others, it is already an integral part of their approach. For example, our survey found that approximately 42% of our respondents already utilize attack surface management. Other key takeaways from our survey include:

- Unknown risk is causing approximately 75% of our respondents to increase their offensive security practices.
- Approximately 58% of respondents indicated that they are satisfied with their ability to identify threat exposure on their attack surface. About 77% utilize ASM findings in their risk management program.
- An ASM program's most significant efficiency metric is the *discovery of misconfigurations and vulnerabilities*, followed by security gaps and shadow IT, respectively.

Furthermore, our survey also represents responses from various industries, geographies, and roles. Figure 1, below, provides a snapshot of the demographics of our respondents.

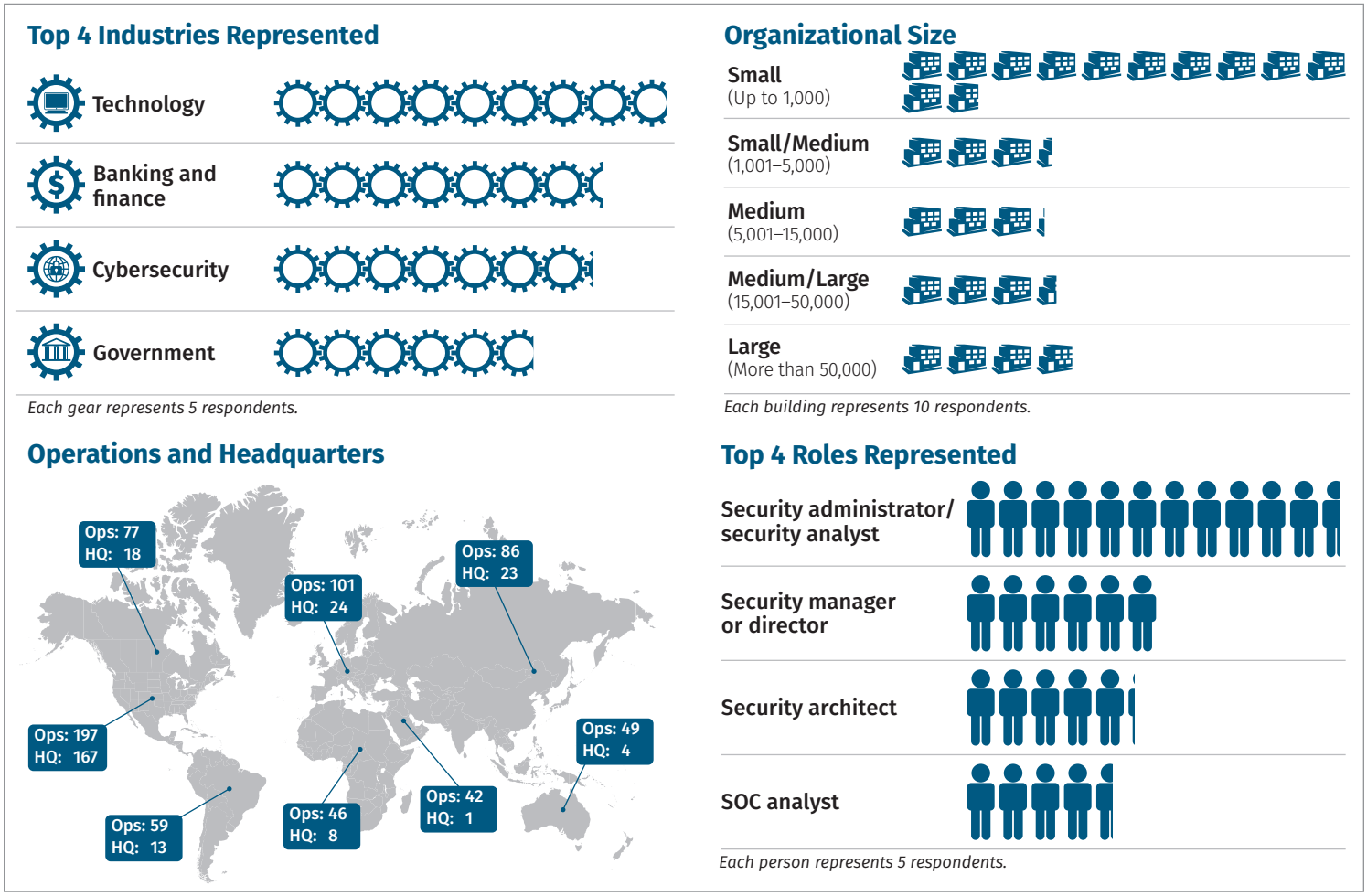

Figure 1. Survey Demographics

Risk Management and Assessment

Our assessment begins with analyzing how offensive security operations play a role in mitigating risk. Actively probing and attempting to exploit vulnerabilities helps provide insight—and knowledge of weaknesses—in an organization's security posture, tech stack, or response processes. This proactive approach can help identify potential threats before an adversary realizes them, allowing for proper remediation.

Furthermore, offensive security operations enable organizations to prioritize risk mitigation efforts with a real-world assessment of how their environment might become compromised. Although proactive security can help mitigate known risks, it can also be instrumental in exposing unknown risks. We found agreement with our respondents, with approximately 75% stating that they increased proactive security practices to combat unknown risks. See Figure 2.

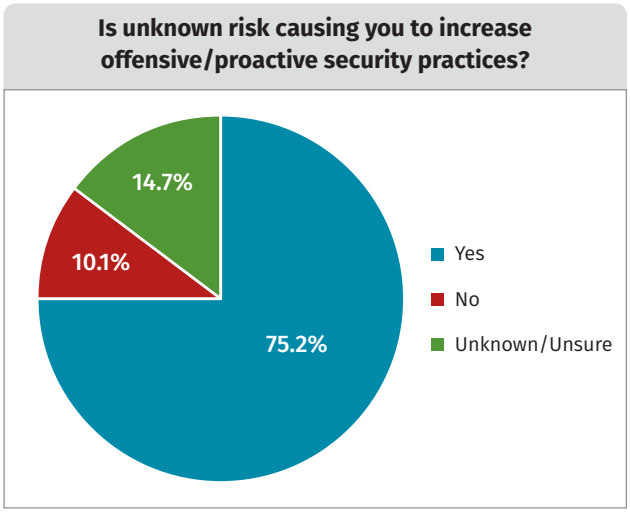

Figure 2. Unknown Risk Influence on Proactive Security Practices

Another consideration is that not all offensive or proactive security operations are identical. Some measures may provide different coverage or insight than others. Consider, for example, a bug bounty program versus automated penetration testing or penetration testing as a service (PTaaS). Both require different skill levels and knowledge of the environment and thus may provide additional insights or feedback. We asked our respondents what different measures they use to identify application security coverage. See Figure 3.

In many of our surveys, for specific questions, we provide an option of "Unknown/Unsure." It is are not uncommon for these answers to constitute a double-digit percentage of respondents. Rather than address them individually, we can provide a blanket statement: If you are unsure of your security posture or operations, we highly recommend gaining that visibility before looking at future implementations or capabilities. Many organizations have overlap in tooling and processes and should look to find efficiencies first.

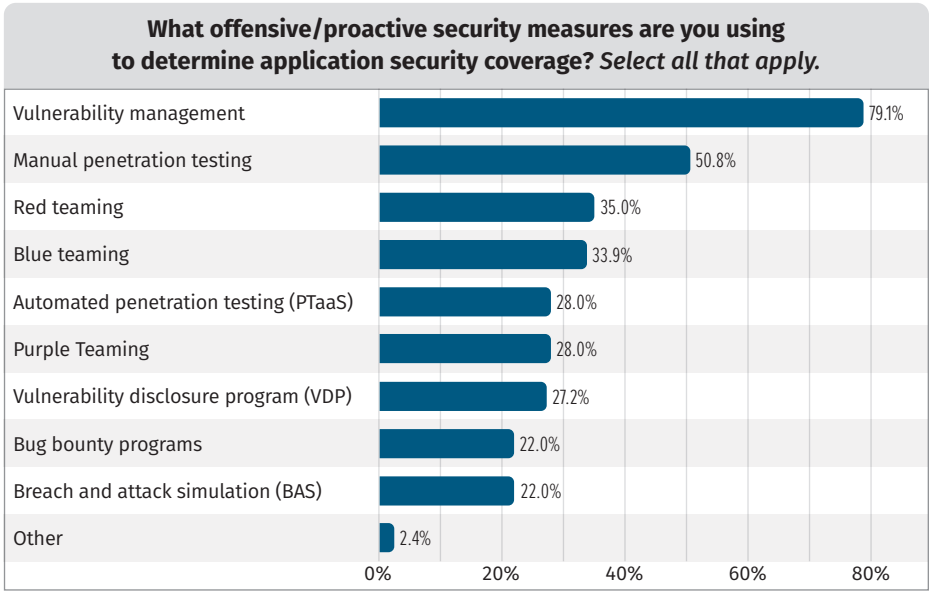

Figure 3. Offensive/Proactive Security Measures in Use

Most of our respondents, approximately 79%, rely on vulnerability management to determine application security coverage. There is a wide gap between this and the second-place response, manual penetration testing at 51%. For us, this emphasizes where organizations are finding the most success. We expected to see "manual" teaming methods, such as red, blue, or purple teaming, have more representation. However, they came in at 35%, 34%, and 28%, respectively. Bug bounty programs were only present within 22% of respondents' organizations. Our key takeaway here is that most organizations rely on vulnerability management rather than other processes and, as stated, find the most success there.

Interestingly, the top four proactive measures in Figure 3 depend on humans. Although a vulnerability scan can be automated, interpreting and acting upon results is largely human-driven. Manual penetration testing relies on the skills of the humans involved, as does blue and red teaming. These three measures rely on the skills of humans to identify vulnerabilities and gaps within a security posture, sometimes catching weaknesses that automated tools might miss. Finally, purple teaming (the sixth top response to this question) is also inherently human-driven, requiring collaboration between blue and red teams.

As mentioned in the Introduction, our survey also wanted to focus on how ASM integrated with threat mitigation and offensive security operations. We first wanted to define whether respondents had succeeded with attack surface management solution(s) and their contribution to threat exposure. Figure 4 has those results.

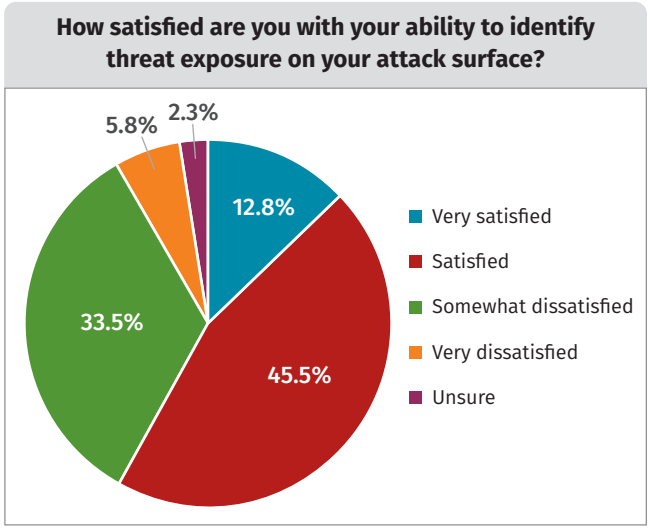

Figure 4. Satisfaction with Threat Exposure Identification

Approximately 58% of respondents indicated they were at least satisfied with identifying threat exposure on their attack surface. Our interpretation is that some attack surface management solution or knowledge is in place—a great starting point! Conversely, dissatisfaction consumed approximately 39% of respondents. This is perhaps a graver figure—a solution is in place, but respondents are unhappy with its contribution to identifying threat exposure.

Another key point is whether ASM data is effectively used, regardless of satisfaction. The adage that offensive security operations end up in a report that "no one reads" does little to add value. Even worse is when adversaries exploit a "known" vulnerability with clear documentation that was ignored. The impact we'd encourage would be to see proactive security operations integrated into security risk management.

For part of our survey, we focused on using ASM within our respondents' environments, looking for their top concerns. After all, top ASM concerns can provide just as much momentum as unknown risks. Figure 5 shows these results.

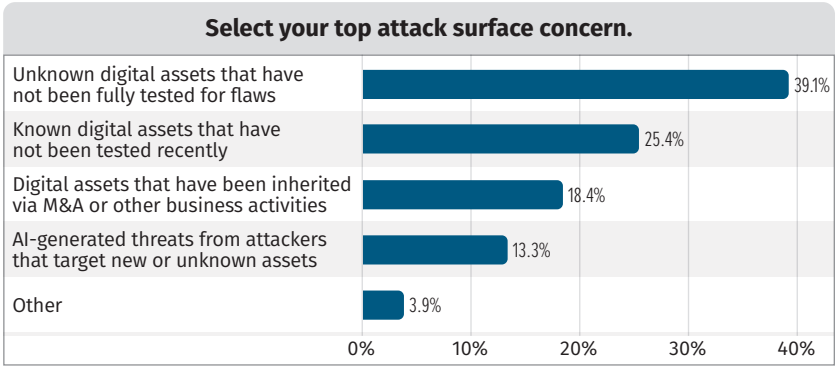

Figure 5. Attack Surface Concerns

Approximately 39% indicated that unknown and untested digital assets are their top concern, with known and untested assets coming in at around 25%. We found it very interesting that only 18% of respondents indicated that inherited assets are a concern—we expected this number to be higher. Some of these concerns are also captured in unknown and untested assets, likely adding more weight to their significance. Only 13% of respondents indicated that AI-generated threats, a new adversary capability on the horizon, contributed to their attack surface concerns.

Risk Mitigation with Attack Surface Management

Although we posit that an entire offensive security strategy is critical in understanding security risks and mitigation, attack surface management provides valuable insight into your exposure. This survey section focuses on whether respondents use attack surface management technologies and how they derive value from those implementations.

EASM in the Enterprise—Who's Using It?

We began by asking if our respondents utilized external ASM (EASM)—helping us understand where these technologies are represented. Figure 6 looks at these results.

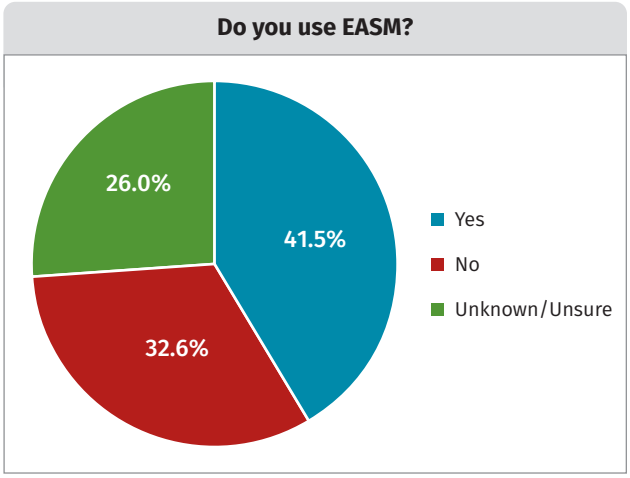

Figure 6. EASM Usage

Less than half of our respondents, approximately 42%, utilize EASM. Given the risks and previously described usefulness of EASM data, we expected a higher representation. Interestingly, more than a quarter of respondents (26%) were unsure. Although we addressed unsure/unknown results earlier, we'd continue to remind security stakeholders to know what solutions are in their environment.

The most significant reasons why EASM wasn't being used were (1) cost and (2) staffing concerns. Figure 7 shows other key contributors, including lack of prioritization of findings, too much data (high false-positive rate), and lack of tooling and integration issues.

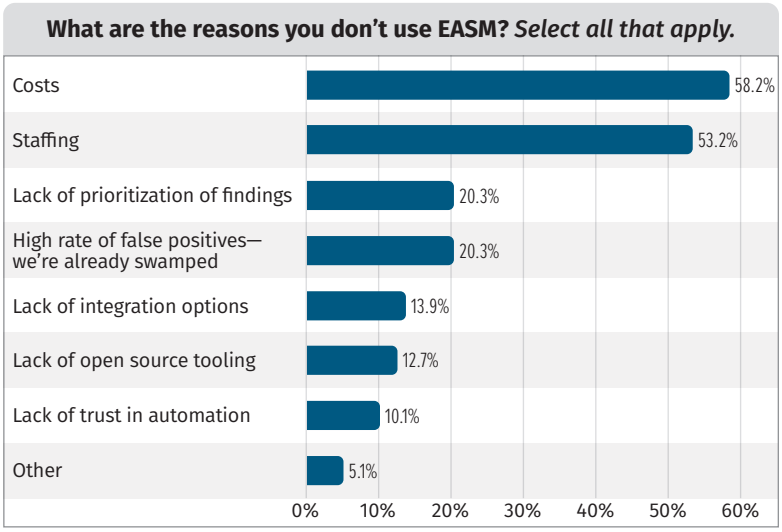

Figure 7. Reasons for Not Using EASM

Although costs and staffing have long plagued successful security processes and tool implementation, we were surprised to see how much they prevailed among reasons for a lack of EASM. We also had one write-in response that captured the sentiments of others—one respondent indicated that their small footprint made EASM cost ineffective. This argument almost feels circular—knowing you have a small footprint is attack surface management. However, we agree that a dedicated tool or platform is only necessary for some environments.

For organizations that utilize EASM, we also wanted to understand what imperatives their EASM results mapped to. See Figure 8.

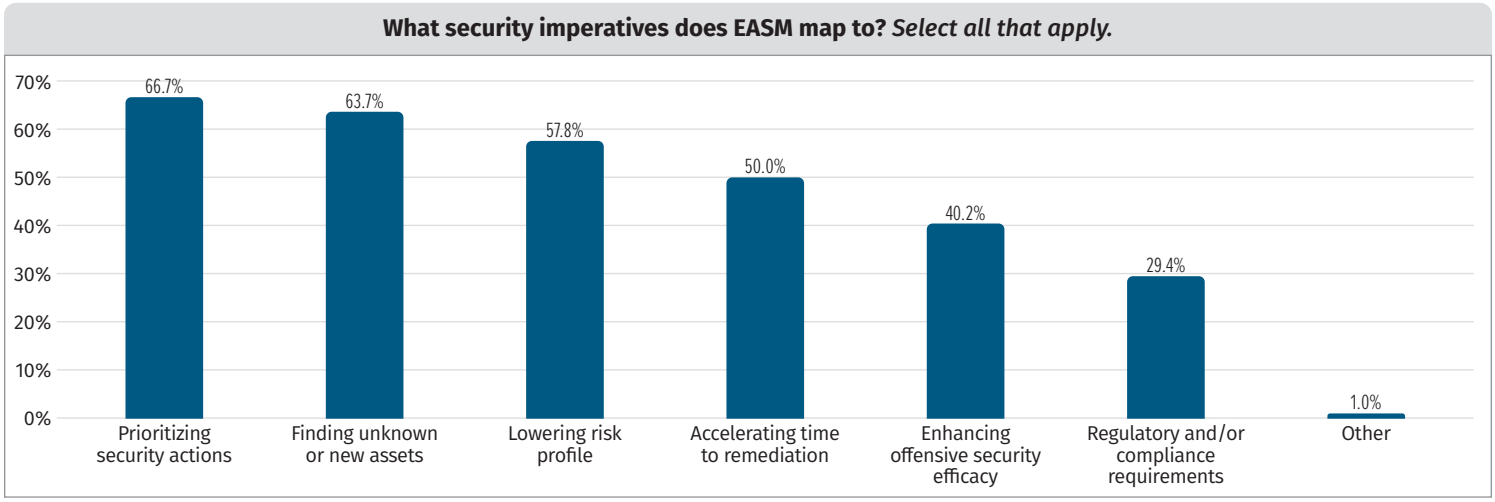

Figure 8. EASM Mapping

Two-thirds of our respondents indicated that they utilized EASM to prioritize security actions. This is precisely what we sought to find out! Taking the second-place response is finding new or unknown assets, a valuable feature of EASM that we could have easily seen be number 1. To round out the top three, approximately 58% use EASM to lower risk profiles, which aligns directly with our hypothesis for this survey.

As we saw in Figure 7 earlier, some organizations stated that cost or lack of open-source solutions were their reasons for not utilizing an EASM solution. However, for those that do, we set out to understand whether they had built their own or used a premade solution. Our respondents indicated that approximately 87% used an EASM provider or custom solution, with a mix of EASM vendors or custom-tool development. See Figure 9.

If you're considering an EASM solution, one of the most important considerations is where the value will be realized within your security program. As shown in Figure 8, it is clear that EASM data contributes to prioritizing security actions, discovering new assets, and lowering risk—things we know every security program wants *and* needs!

Of those respondents using a provider or custom solution, most (61%) used an EASM vendor. Approximately 41% used a custom tool that was developed in-house. Note that we let respondents select all answers that applied, so it is likely that we're seeing a crossover of vendor-provided and custom tooling to achieve EASM needs. Approximately 22% indicated that they were using manual processes. Although this may seem archaic to some, we will always argue that progress is progress, and manual processes are a step in the right direction!

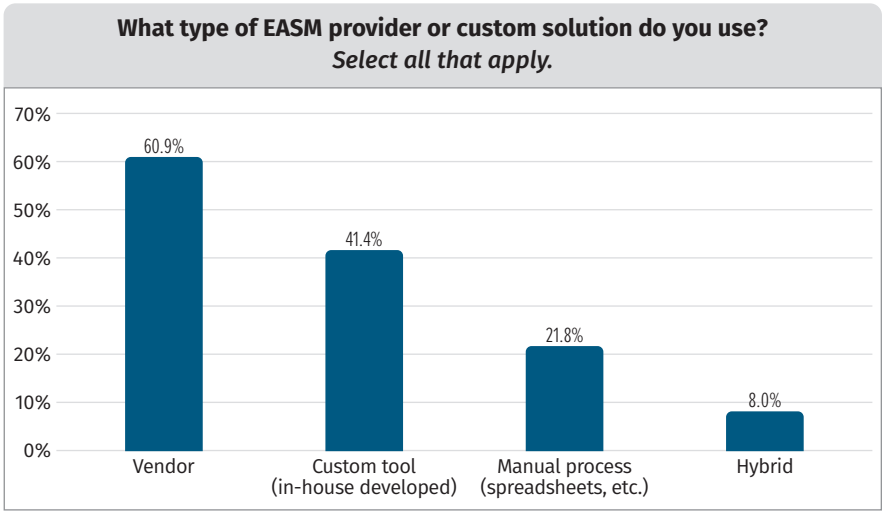

Figure 9. EASM Providers/Solutions

EASM in the Enterprise—Efficacy

Having an EASM solution in place is only half the battle. The other consideration is whether the solution is performing effectively. We asked our respondents—do you measure the effectiveness? A resounding 74% came back and said yes. We pressed on and asked how one measures the effectiveness of an EASM program. See Figure 10.

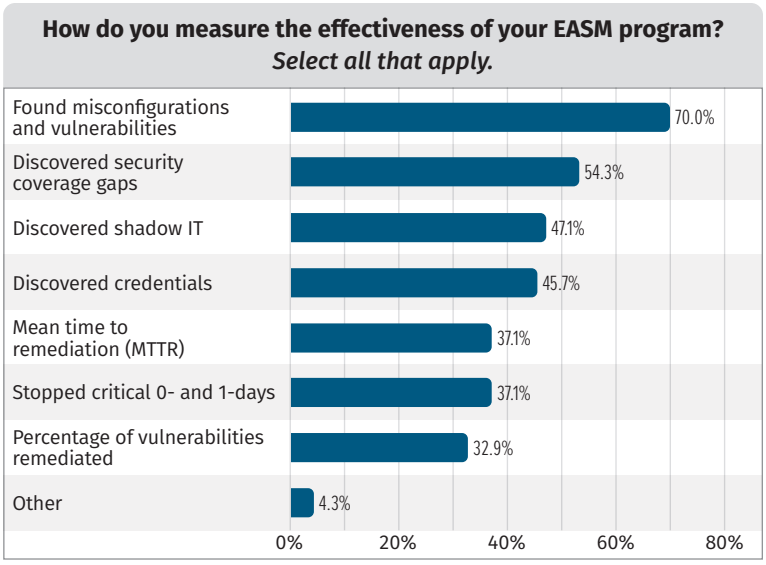

Figure 10. EASM Efficacy

Our respondents proved that the efficacy of EASM can be evaluated with a simple question: Do we know what we don't know? From the results above, the top four results came out as:

1. Found misconfigurations and vulnerabilities (70%)
2. Discovered security coverage gaps (54%)
3. Discovered shadow IT (47%)
4. Discovered credentials (46%)

It should come as no surprise that, when an EASM solution is put to the test, its output is central to its efficacy. We feel that the efficacy of EASM is instrumental in achieving substantial reductions in threat exposure. By identifying and managing their external attack surface, organizations can minimize their footprint and limit adversary entry vectors.

SANS strongly encourages proactive security measures, including utilizing any and all data to help secure your networks. With ASM data in hand, organizations have a "leg up" on adversaries and should put these findings to the test.

We'd go as far as to suggest that this should be a metric for any organization using an EASM solution or looking to evaluate efficacy. Ask yourself: Did you see a reduction in risk, or more proactive activities? Consider what your team has done with and without EASM data, and determine if your security posture has become more forward-looking.

However, EASM implementations are not perfect. This should not be a deterrent, but rather a chance for improvement or careful assessment during the POC stage. Approximately 69% of respondents indicated that they *did* have challenges with an EASM solution, ranging from too many results to lack of effective AI (see Figure 11).

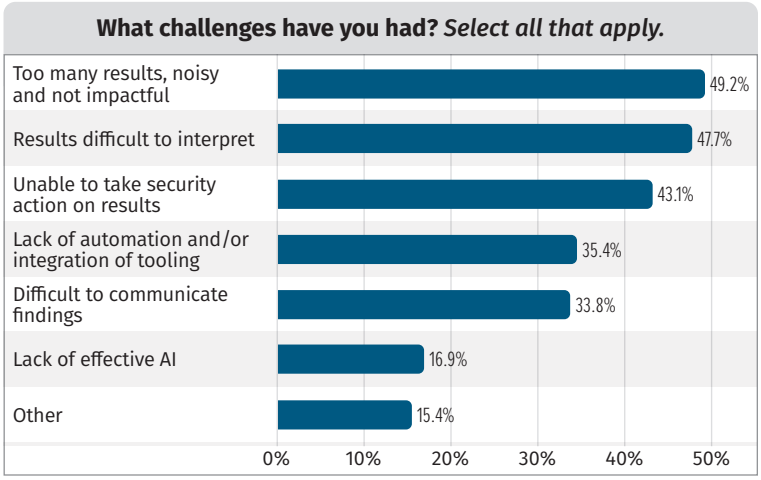

Figure 11. EASM Challenges

Earlier in our survey results, we explored that a high rate of false positives is a key contributor to why organizations don't use EASM. Not surprisingly, the number 1 complaint is too many noisy results. Nearly 50% of our respondents indicated that there are too many results, while a close 48% indicated that results are difficult to interpret.

The key takeaway here? EASM vendors and implementors have an opportunity to help streamline and refine results so they are easier to consume and evaluate. Many organizations *want* EASM capabilities, but they must make sense first.

EASM in the Enterprise—What Would You Look For?

Given that many of our respondents utilize and find value in EASM solutions, we explored further what constitutes those solutions. After all, not all environments are made equally, and neither are the tools that support them. This section looks at respondents who currently did *not* have an EASM solution in place—we wanted to understand what value they seek. See Figure 12.

Not surprisingly, the most common factor is integration with a current security tech stack, coming in at just over 72%. This representation makes sense—EASM solutions are often built to augment or renovate an existing tech stack, not as a cornerstone of defense, like other products (i.e., endpoint detection and response [EDR], network detection and response [NDR], or SIEM tools). What was surprising was that the breadth of discovery came in at approximately 46%, fourth place in our list of factors. At the onset of this survey, we expected that integration and breadth would be contenders for the top two positions.

We also asked respondents which capabilities they found important in an EASM solution. Given the answers to previous questions, vulnerability identification at approximately 77% was no surprise. See Figure 13.

We've seen other questions lead toward vulnerability discovery and management as a critical element of EASM, and multiple results support this thought. Figure 13 confirms that for us. Rounding out our top three at 66% each are continuous discovery and continuous monitoring. Comprehensive digital asset inventory was desired by approximately 53% of respondents, which lands closer to the "asset" side of EASM versus vulnerability discovery.

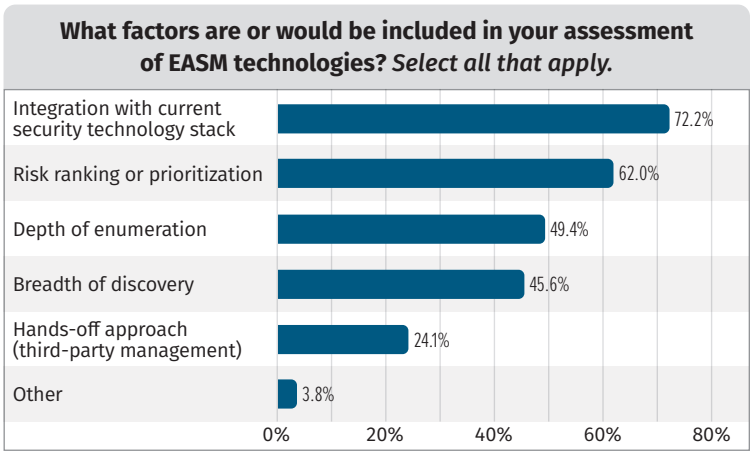

Figure 12. EASM Assessment

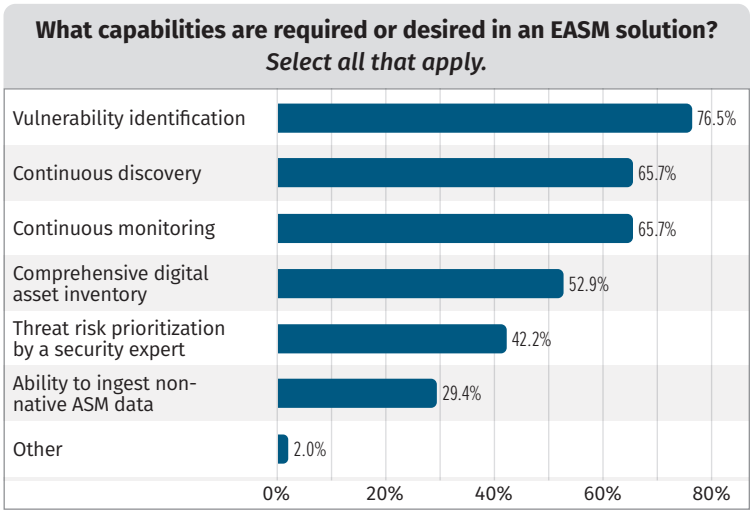

Figure 13. Necessary EASM Capabilities

Speaking of the "asset" side of ASM, no tool or solution should ignore that inventories of assets *and* vulnerabilities are components of a successful solution. Our respondents agreed when we inquired about what types of asset attributions they need their EASM solutions to identify. Our results represented what we feel is today's modern enterprise (see Figure 14).

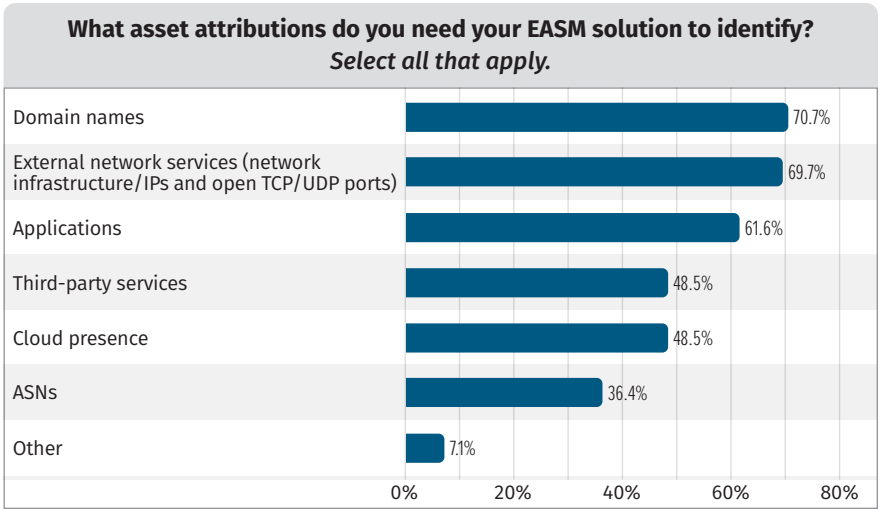

Figure 14. Desired Identification of Asset Attributions

The results show that our respondents understand their vast digital footprints, ranging from cloud presence to third-party services, applications, and external network services. However, we found it interesting that the top response (albeit by 1%) was domain names, at 71%. From an attack surface perspective, this can go two ways. Domain names may not serve as attack vectors, but the relationship between a single entity and various other domain names would undoubtedly arise during adversary victim reconnaissance.

The number two position, "external network services," at approximately 70%, caught us by surprise. We expected it to hold the number one spot. Remember that EASM looks to profile your *external-facing* footprint and profile those applications and their potential vulnerabilities. Rounding out the top four were applications and third-party services, which are asset types we view as essential for EASM reporting.

Finally, we also asked our respondents about the future of EASM concerning their current tech stacks. Most important: Do they plan to incorporate EASM in their security processes in the next 12 months? Figure 15 shows us that many organizations (approximately 51%) are undecided or neutral in the decision.

The most significant takeaway from these answers is that approximately 23% of respondents will likely include EASM in their security processes. For the approximately 27% who said *unlikely* or *definitely not*, we'd encourage you to examine where and how EASM solutions can complement your current processes. Your security team may have a gap or risk exposure simply because the digital footprint has yet to be classified.

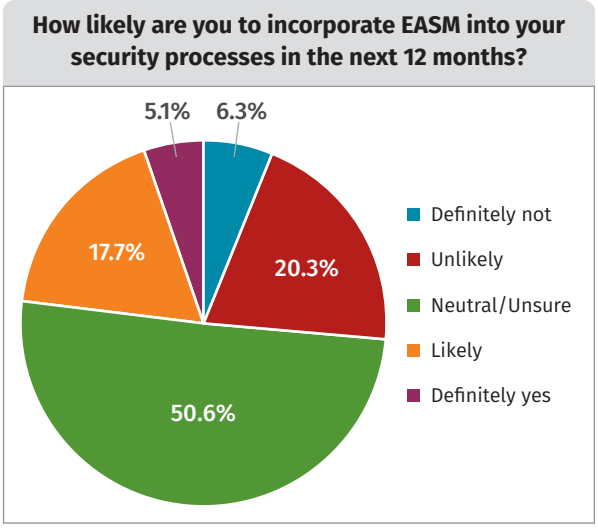

Figure 15. EASM Addition in the Next Year

Closing Thoughts

Imagine an environment where security teams have zero insight into their attack surface or the tactics by which an adversary might compromise their environment. It's impossible to ignore how valuable this knowledge is to one's security posture, especially regarding enterprise exposure and risk. In this SANS survey, we spent time with our respondents to understand precisely how these activities translate to risk management and mitigation.

Part of our survey focused on the use and value of attack surface management (ASM) concerning offensive security strategies. ASM is integral to any strategy, and the technology will strengthen. Furthermore, integrating AI and automation will be another step in the right direction, providing analysts with more detailed and precise attack surface mappings.

Today's organizations are vaster than ever, with hybrid environments that depend on third parties, software supply chains, and external-facing services. We've seen repeatedly that not understanding one's attack surface creates massive gaps for adversaries to walk through. Furthermore, an offensive security strategy that fails to capture the unique details of an organization does little to help bolster an organization's security posture, and attack surface management is a large part of building that education.

Tomorrow's security teams will find success in incorporating and acting on as much knowledge as they can to remain well-prepared for any threat that comes their way.

Sponsor

SANS would like to thank this paper's sponsor:

hackerone