National Cyber Security Centre
a part of GCHQ

ACTIVE CYBER DEFENCE 2.0

Attack surface management experiments

March 2025

Contents

Introduction

ACD2.0

In August 2024 the NCSC's CTO Ollie Whitehouse and Director of National Resilience Jonathon Ellison signalled the next stage of the NCSC's Active Cyber Defence (ACD) services with the announcement of ACD2.0[1]. The core approach for ACD2.0 is that of partnership; across the NCSC, across the cyber security community in government, and crucially also with industry and academia. The journey started with the first series of experiments exploring attack surface management (ASM).

Following that announcement, a small time-bounded team was formed to formulate and carry out the ACD2.0 ASM experiments over the following six months. In January, we shared our initial insights and thanked the ASM providers for their involvement in this work[2].

This report is a deeper dive into what we have learned. The project itself was a set of experiments, but we have focused this report primarily on the **Commercial Trials of EASM Products & Services** experiment, where we believe there is the most benefit to an external audience.

Experimental approach

We have referred throughout this work to running experiments, or taking an experimental approach. This concept was a fundamental value in our approach to this work. We were robust (including with our internal stakeholders!) in defending our position that we would not pre-judge the outcomes of this work until reaching the final conclusions, and that any conclusions and recommendations would be grounded in evidence from our research.

Why ASM?

Attack surface management was chosen as the first of the ACD2.0 experiments for a variety of reasons. This was not least due to the NCSC's years of experience running ASM or ASM-like services – namely Web Check, Mail Check, and Early Warning.

The experiments were under the banner of ASM. However, the focus of this report is on our commercial trials specifically of **external attack surface management (EASM)** products. For the purposes of this experiment, we defined an EASM product as something that:

> *"conducts or uses scanning data to identify assets or services that are publicly reachable online and highlights risks associated with the asset, its configuration, or maintenance"*

[1] https://www.ncsc.gov.uk/blog-post/introducing-active-cyber-defence-2

[2] https://www.ncsc.gov.uk/blog-post/active-cyber-defence-2-easm-update

Objective

The primary aim of this experiment was to **gain better market understanding** with a view to understanding the benefits of EASM products, market differentiators, approaches to risks and authorisations, and considering future commercial models.

We sought specifically to understand:

- the extent and maturity of the commercial market
- the cyber security benefits of using EASM products
- the types of solutions and features available
- where the NCSC's role as the National Technical Authority (NTA) best fits

Additionally, as the first of the ACD2.0 experiments, we aimed to:

- understand the best way to carry out these partnership-led experiments
- challenge internal NCSC ways of working to allow the experiment to maintain independence
- make recommendations for how we run the next ACD2.0 experiments

Key findings

Throughout this report, we have highlighted where we have drawn specific conclusions used to inform our recommendations. Some of those are summarised here:

- **There is a clear established and thriving commercial market for EASM, providing quality services at a range of price points (including some free tiers).**
- There is no concept of a one-size-fits-all EASM product.
- Users gain direct and/or indirect cyber security benefit from a range of EASM features.
- Providers are very keen to work with the NCSC and will act quickly and flexibly to do so.
- A wide variety of loosely defined language is being used to describe scanning activities.
- Customer organisations routinely raise concerns about potential impact of EASM scanning activity.

Gaps and opportunities:

- There is a gap for authoritative leadership in identifying what specific EASM-related risks and issues are most critical for organisations to resolve.
- There is a gap for authoritative leadership on what constitutes a good EASM product and how organisations should go about selecting one.
- There is a gap for thought leadership regarding responsible monitoring of 3rd parties using EASM and related tools and products.
- There is an opportunity to establish a better connection with the industry to share our leadership as an NTA, keep up to date with developments, and build a view of what is happening across sectors to ultimately serve end users better.

We have made internal recommendations for the NCSC to address the key gaps identified. Subsequent announcements and publications will be made as appropriate.

Methodology

To achieve the primary aim of better market understanding, the experiment involved the following activities:

- asking EASM providers to offer free trials and agree to help with our research
- signing up a selection of customer organisations to the free trials
- observing the use of the products
- interviewing providers
- surveying and interviewing customer organisation users

The trials

In numbers, the commercial trials included:

- 10 EASM products
- 27 customer organisations
- 35 trials (some organisations trialled multiple products)
- Around 900 days' worth of combined trial time
- Average of 25-30 days per product per organisation

Working with providers

We published a public call to EASM providers to be involved in the experiment, asking for low- or zero-cost proposals. The response was very encouraging, with 20 companies making offers. Due to limited team bandwidth, a selection process was conducted to limit the trials to 10 products. This review included alignment with our definition of EASM, previous NCSC engagement, flexibility of the offer (noting any caveats), and primarily **ensuring technical diversity of EASM solutions** within the trial.

Because this selection was not a rigorous formal commercial process, it must not be considered a reflection on the quality of products or services from the organisations. The NCSC publicly acknowledges and thanks all companies who offered to work with us on this experiment.

Throughout the experiment, the support and engagement offered by the EASM providers was excellent. They were keen to help us, made plenty of time available both directly to us and to the onboarded customers, provided insightful feedback in interviews, and were highly responsive to our requests. We felt that providers appreciated the opportunity to shape the NCSC's direction, and provided valuable input – we recommend this approach be considered for other ACD2.0 experiments and wider.

Conclusion – Providers are very keen to work with the NCSC, and will act quickly and flexibly to do so, even incurring costs to support experiments.

Working with customer organisations

We recruited volunteer organisations through various methods to achieve a mix of public and private organisations of various sizes.

We will not publicly name the participating organisations, but would like to take this opportunity to thank all those who gave up their time and resources to support our experiment.

One observation worth highlighting was that several organisations had concerns over scanning activities carried out by EASM products, with several requiring security sign-off or approval from change boards. This was more common in larger organisations. In contrast to the provider engagement, where we were concerned that asking for free product trials would be a blocker but had a very positive response, **we found giving away those free product trials was a much bigger challenge**. The time spent discussing concerns and resolving issues impacted our onboarding timelines and limited our experimental data collection. This is not a criticism of the participating organisations, but rather an observation of the challenges in understanding the risks of scanning, something we explore later in this report.

Conclusion – It was easier to get EASM providers to offer free trials to support the NCSC's experiments, than it was for customer organisations to onboard onto those trials.

Matching providers and customers

We made best efforts to match customer organisations to EASM products to achieve the following, often contradictory, principles:

- ensuring a mix of organisation types (public/private/charity) on each product
- ensuring a mix of organisation sizes on each product
- managing the organisations' risk appetites
- making sure organisations got cyber security benefit from the work, by picking EASM products best suited to their current challenges

Marketplace understanding

This section details the knowledge gained and conclusions formed about the external marketplace from our trials. It should be caveated that this insight was gained from limited experience with ten EASM products for a short period of time. Whilst we believe that common conclusions across more than half of these products likely hold true across the whole market, those with fewer examples may be outliers.

This section has the following outline:

General features

It is clear from our market trials that features and user experiences vary considerably across the various EASM products observed. Such variations arise from tailoring to different customer sets, focusing on specific technology areas, providing unique selling points, and differing philosophies and approaches to the problem space.

We categorise common EASM features into three groups below.

Insight/visibility

Features which provide attack surface visibility, that users can directly use, or interrogate to identify anomalies.

- Asset discovery
- Technology identification
- Service identification
- DNS configuration
- Web presence
- Brand protection
- Supplier identification

Security analysis/issues

Analysis of the attack surface usually leads to raising of risks or issues for action, often with remediation advice and explanatory references.

- Email security
- Web security
- DNS security
- Software security
- Exposed services risks
- Vulnerability assessment
- Threat intelligence

Supporting functions

- Workflow features
- Configurable prioritisation
- 3rd party integrations (eg SIEM, workflow tools)
- Raw data exports (eg CSV download)
- Summarised reporting features (eg PDF download)
- Dashboarding
- Scoring/health metrics
- Hierarchical organisational access control

Feature configuration

For almost all EASM products observed, any supported features from the above list are integrated into a single product offering, and are enabled by default. In some cases, different subscription tiers unlock additional features. But in almost all cases, if a feature is available, it is applied automatically to all relevant digital assets without requiring user configuration.

Vulnerability assessment is an exception where it often requires specific switching on and configuration, particularly in cases where this involves more intrusive scanning such as 'payload analysis' (see: Language of scanning).

Where relevant to the conclusions of this report, some of these features are considered in more detail in the following sections.

Value of features

This report will not attempt to compare the value of specific features of different EASM solutions. We did not have sufficient sample size of customer organisations to make a statistically significant assessment of features across all trialists. However, we were able to observe and discuss with organisations some examples of security benefit obtained through the trial.

The direct link between features in the 'security analysis/issues' category and cyber security benefit is the most clear – people are made aware of bad things and they fix them. However, we observed that customer organisations got either direct security benefit, or increased actionability and response speed, from other features.

Some examples of these cases:

Discovery – one organisation was made aware of several legacy websites they thought had been decommissioned but were still live, which they then took down. Multiple organisations benefited directly from asset discovery – this will be looked at in more detail.

Web presence – one organisation used a feature showing screenshots of external webpages to identify a bug in a service that should appear differently to internal and external access.

Brand protection – an organisation identified additional domains they had not enlisted when their branding was identified on a forgotten recruitment website.

PDF exports – used by one customer to forward on to the team that controls the service at risk, so they could take action to mitigate it. The same organisation said that it was harder to action the findings from a different EASM which lacked this feature. **CSV exports** were used similarly by other organisations with a larger number of risks.

Workflow features – used by one customer with multiple organisations to leave comments between each other, making it clear who is actioning what.

Conclusion – Users gain direct or indirect cyber security benefit from a range of EASM features, outside of being presented with specific risks and issues data.

Conclusion – Many commercial EASM products invest significantly in development of feature-rich user interfaces grounded in user research. Most consider the UX a core part of the value of the product (not just the data). Users' EASM needs differ and so cyber security benefits are gained from different features.

Asset discovery

Across the EASM products, the different approaches to asset discovery have two main distinguishing factors: the type of seed data, and whether discovery is automatic or produces suggestions that require manual confirmation. Some EASM products merge different approaches.

Seed data

Seed data takes two forms: **technical**, or **commercial**.

Technical - in these cases, customers provide a seed list of known technical identifiers (typically domain names and/or IP addresses) related to the organisation from which the solution performs discovery. This is the most typical type, which was supported by almost all EASM solutions trialled.

Commercial – in these cases, discovery is seeded by the organisation's name. This is most common for solutions in the market space focused on managing 3rd party supply chain risk. It is also used as additional seed data by some EASMs.

Automated or suggested

When discovering additional assets, a solution can choose to present those to the user as suggestions, or silently incorporate them into the considered digital footprint of the organisation.

The vast majority of discovery observed across all products was automatic, with any risks and issues being immediately raised against any assets whether part of the seed list or discovered. In most cases, discovered assets are transparently included in all data, but kept separate from the initial seed list. This allows discovered assets to be transient, which is important for things like IPs resolved from linked domain names.

No EASM solutions distinguished between primary domains and subdomains when it comes to discovery. For all products, adding the primary domain as an asset was sufficient to include all known subdomains within the analysis.

The only observed examples where manual confirmation was required was where products suggested potentially related primary domains based on key word matching. In all cases, this was in addition to transparent automatic discovery.

Conclusion – All EASM solutions consider any subdomains of a domain owned by an organisation to be automatically in scope for monitoring.

Discovery techniques

There are a wide range of techniques used for discovery by products, with different providers having varied opinions on whether techniques are commercially sensitive. One provider commented that "*discovery is a commodity service now*", whereas another claimed they "*have the most comprehensive list of domains on the internet of anyone*", and yet another that "*Asset discovery is one of our key differentiators. There is no other vendor in the ASM space who does it better*".

Some common techniques include:

Most EASMs:

- discover subdomains via various sources including Certificate Transparency Logs (CTLs) and passive DNS
- resolve all domains (including subdomains) to get IP addresses
- identify additional domains from other DNS record types (e.g. MX)

Some EASMs:

- interrogate SPF records to acquire more domains and IP addresses
- analyse certificates for additional related primary domains
- perform reverse DNS on IP addresses
- match domain or IP WHOIS information against an organisation

Few EASMs:

- use global scanning to identify additional domain names resolving to known IP addresses
- use additional open source company information to identify domain names

In most cases, discovery is a recursive and continuous process whereby multiple techniques can end up being chained together.

Some EASM products are transparent about the provenance of discovered assets, including by which technique they were discovered; however, the level of detail varies considerably. **We observed a lack of transparent provenance detail negatively impacted the actionability of risks related to discovered assets**.

Presentation of discovery results

Most EASM products provide a view within the user interface presenting the entirety of the organisation's assets. This is referred to differently by different tools, as:

- attack surface
- assets / external assets
- inventory
- footprint
- referred to purely as 'domains or 'IP addresses', or 'hosts'

Within the trials, we observed that some customer organisations gained significant value purely from this step of the process – having visibility of their full list of discovered assets.

This included:

- identification of legacy domains they thought had been decommissioned
- realisation that domains they didn't consider public were discoverable
- identification of new services the cyber security teams didn't know about

These all have direct mapping to security benefit, by providing visibility of the existing state of the attack surface, allowing security teams to kick off new work to protect new assets or complete decommissioning of old ones.

Conclusion – There is cyber security benefit in providing visibility of the digital footprint of an organisation (eg all domains and IP addresses), particularly when paired with high performing asset discovery.

Discovery performance

Customer organisations in the experiment provided their initial seed domains and IPs. For domain names, we only provided primary/apex domains to EASM providers (not subdomains), to enable products to perform their own discovery.

As an example, one charity organisation trialist had just one domain with one additional subdomain in their MyNCSC asset portfolio. The EASM product discovered nearly 250 active subdomains. In another case, for a large private organisation, over 70 new IP addresses (+44%) and 80 domains/subdomains (+250%) were discovered.

We did not focus on direct comparisons between EASM products. However, we did make some discovery coverage comparisons where possible. We found evidence when comparing products that it was rare that a single product outperformed conclusively. Instead, each product discovered some assets missed by the other – however the majority were found by both.

Anecdotally, organisations commented on impressive discovery coverage of their assets across the majority of EASM providers, including comments such as "*I don't know how they found out about those domains*". No organisations raised any concerns that known assets were not discovered.

Conclusion – Almost all EASM products perform some level of automated asset discovery, using a variety of techniques. Whilst technical performance coverage varies, all observed discovery was sufficient to provide visibility perceived as comprehensive by customers.

Suppliers and 3rd party risk

EASM products

There is a marked difference in the EASMs we looked at between the approaches towards monitoring of digital assets **that the customer does not own** or have authority for.

They broadly fit into one of four categories, on this scale:

Not allowed (customer must own assets)	Allowed	Allowed, and have specific features for 3rd party assets	Primarily tailored for looking at 3rd parties

More and more EASMs appear to be adding features to allow 3rd party monitoring, as well as several products existing entirely for this purpose. The NCSC has existing guidance highlighting the increasing importance of supply chain security[3], however does not currently consider the application of EASM products to identify and manage supply chain risk. There is a lack of thought leadership and guidance on what a responsible approach to 3rd party monitoring should look like – from the perspectives of customers, EASM providers considering features, and suppliers potentially being monitored.

Conclusion – There is a gap for thought leadership regarding responsible monitoring of 3rd parties using EASM and related tools and products.

Hierarchical access control

One feature found in a few EASM products is the ability to manage organisations in the tool through hierarchical parent/child accounts. This can provide a parent organisation with visibility of EASM data for a set of child organisations over which they have some security responsibility or provide some security services. An example might be an organisation responsible for an entire sector provisioning EASM accounts for other organisations, whilst maintaining visibility across the full sector attack surface. When scaling the benefits of EASM, this feature enabling a 'defender community' model may prove valuable.

Conclusion – Some EASM products provide features such as hierarchical accounts that would support deployment in a defender community model.

[3] https://www.ncsc.gov.uk/collection/supply-chain-security

Product tailoring

From these trials, we see a tailoring of products for differently sized and skilled organisations. There is a marked difference between products targeting large enterprise customers, and those catering for smaller ones. We also observed different EASMs offering more or less value for organisations facing particular types of problems and security challenges.

During this work, we found ourselves able to suggest different products based on an organisation's specific situation. For example, if an organisation is primarily concerned with vulnerabilities in their web applications, we suggested a different EASM than if they are in the process of decommissioning domains and need visibility of their namespace. Similarly, for organisations with a large number of IP addresses wanting to understand exposed services, there are EASMs that are particularly strong in that space; versus ones that work well if organisations want to take a more compliance angle, or organisations that require integrations into existing workflow tools.

In many cases, EASM products have similar data, but the ways they interpret, analyse, collate and present to the users make fundamental differences to the products, what problems they best solve, and how usable they are to different organisations.

This is supported by user research, with quotes such as:

- "I think both solutions complement each other and have their own strengths"
- "[Provider 1] was nice but didn't bring any value to us, where [Provider 2] was spot on for our specific work"

Conclusion – There is no concept of a one-size-fits-all EASM product, and we see considerable tailoring in the commercial market.

Risks and issues – identification and prioritisation

The severity ratings of specific security risks varied considerably between tools. In some cases, this is due to providers' own opinions on particular issue types or attempts to highlight specific actions. Some general trends we observed were:

- Because **there is no authoritative source for severity or risk levels**, each provider must make their own judgements.
- Organisations are most likely to only act on issues deemed to be serious, which drives a motivation to err on the side of higher severity/impact ratings.
- EASM products are motivated to show value, which could drive a tendency to classify more risks as serious.
- The use of CVSS scores for CVE vulnerabilities can lead to inflated risk assessments..

The lack of an authoritative source for EASM-related issues was a theme arising from approximately half of our provider interviews, with a strong call for **the NCSC to use its authoritative and independent voice to persuade people that the types of security issues being identified are important to note and action**.

Example points from EASM providers:

- Bringing focus onto issues that aren't CVEs – it's not all about CVEs.
- People are overwhelmed by marketing or previous bad experiences.
- The NCSC should encourage people as to what they ought to be doing.
- Education, education, education.
- Guidance! About what actually matters. Large companies are ignoring risks because its poorly understood.
- We want to say – "you don't have to believe us, go to the authoritative figure of NCSC".
- Not the detail, it's about the concept and the level of importance.
- If we had the perfect explanation no one would leave this stuff out there. Need someone to say trust me you should fix it.
- "There is no vocabulary in people's heads for what we deliver."
- Customers want to know what to do – it's not enough to just say the issue - customers want help to fix it.
- NCSC role is to educate the market and the industries, depts and ALBs we work with on WHY it is important.
- "Tools can point people in right direction and NCSC tells us why it is important"

It is interesting that this request is coming from EASM providers themselves, who in many cases are selling their own version of this information. Clearly, there is a desire for an independent, trusted opinion to reference.

This is further supported by research showing that the NCSC's involvement in the trial made a difference in the ability of trial organisations to actually fix the issues identified, with one participant noting how this helped convince decision makers: "*this is just what I needed to '[encourage] them.' I could then say 'working with the NCSC we've been alerted to the following…*'".

Conclusion – There is a gap for authoritative independent leadership in identifying what specific EASM-related risks and issues are most critical for organisations to resolve.

Conclusion – The NCSC's backing of the trials effected change in organisations that wouldn't have happened without security teams namedropping the NCSC.

Summary

This section has outlined some of the key learning about the EASM marketplace from our EASM product trials. It is clear there is a well-established private market for EASM products, and that this market is providing high value products with diverse approaches, features, and target audiences.

Conclusion – There is a clear established and thriving commercial market for EASM, providing quality services at a range of price points (including some free tiers).

Further Analysis

This section includes areas in which we carried out further research and analysis regarding the NCSC's role in the market, or other cross-cutting themes such as the language used to describe scanning activities by EASM providers.

We explore:

- **The NCSC and the commercial market**
- **Risk understanding and appetite**
- **Future of EASM**

The NCSC and the commercial market

The analysis so far shows there is a well-established market providing quality EASM products that are tailored to different organisation types/sizes and have strengths for different cyber security challenges. We have identified gaps for authoritative leadership that the NCSC could fill as the NTA, for example around risk ratings to support and shape the industry.

There exists a clear challenge for organisations to select the most appropriate product for their needs, and a gap for authoritative leadership on what constitutes a good EASM product.

User research articulates the identification of this problem from both the customer and provider angles:

> "*I believe the NCSC has a vital role to play in shaping the future of EASM and supporting organisations like ours*" - Customer
>
> "*Having good guidance what customers should look for in an EASM. Every deal was uphill trying to convince customers this was a problem to solve*" - Provider

Providing EASM guidance

EASM providers are looking to the NCSC to educate organisations on what is important and what EASM means for them. Providers find their customers are often overwhelmed by different offerings and information, they do not know who to listen to or who to trust, or they don't think a problem will impact them – especially those with less cyber security expertise. They are aware some organisations have had bad experiences with other EASM providers and are looking to the NCSC to be an unbiased and trusted voice. The NCSC holds that authority for their customers and there is a collective desire to be able to point them to us to help them understand if they have a problem to solve - "*you don't have to believe us, go to the authoritative figure of NCSC.*"

When discussing their expectations of the NCSC and EASM offerings, organisations prioritised the requirement for guidance and best practice advice to support them in choosing the right EASM solution. Users feel that "*developing and sharing comprehensive, actionable guidelines for implementing and maintaining an effective EASM strategy would be invaluable*," and not only would this benefit the individual organisations, they believe this would help "*drive broader advancements in the EASM ecosystem, ensuring it remains accessible and effective for all*," and hope this would "*encourage* *providers to maintain high-quality offerings*." Organisations see the NCSC as an authoritative voice to inform their decision making, reinforce their recommendations to leadership, and drive action.

Endorsing products

The NCSC has an established mechanism for assuring products and services[4], which we explored within this experiment. Given the technical variety of different EASM products, we concluded that it would be challenging to design a formal assurance scheme initially from scratch. However, there is scope for establishing a set of principles for EASM products that providers could self-certify against. These principles could also link to any work the NCSC does to address the identified gap for leadership regarding the severity ratings of specific issues – for example by creating a minimum set of risks that a good EASM would be expected to identify.

Conclusion – There exists a gap for authoritative leadership on what constitutes a good EASM product and how organisations should go about selecting one.

Collaborating and knowledge sharing

As previously concluded, providers are keen to work with the NCSC, and will act quickly and flexibly to do so. There is desire for "*working together to solve a problem and showing value through actionable information*" as well as the understanding that the NCSC "*have access to a large amount of threat intel that others don't. Collaboration on that would be helpful. Beneficial for end customer as well*". There is something to be explored in how we best share this knowledge and collaborate to give the fullest and still unbiased view for all end users, whilst maintaining our own knowledge as the NTA for cyber security. The NCSC learned a great deal from working closely with EASM providers in this experiment, and found this a very valuable part of our activities. We recommend future experiments engage closely with industry too. Providers offer unique perspectives on ASM and bring real world examples to share, and they are also looking to us to use our NTA position for leadership.

Conclusion – There is an opportunity to establish better connections with industry to share our leadership as an NTA, keep up to date with developments, and build a view of what is happening across sectors to ultimately serve end users better.

Risk understanding and appetite

Customer concerns

In our efforts to establish the product trials, many organisations raised concerns about the risks of adopting an EASM, particularly regarding scanning. There was uncertainty around the impact of the scanning and a desire to involve more people in the process to manage the perceived risk of scanning.

[4] https://www.ncsc.gov.uk/section/products-services/all-products-services-categories

Organisations often don't realise that they are already regularly being scanned by a range of actors, or could be at any moment, regardless of their approval. The real risk lies in the consequences of putting something on the internet, which seems to be poorly understood.

Language of scanning

We observed that the language used by different cyber security solutions and related organisations to describe the process of gathering data about the external attack surface of an entity varied tremendously.

Scanning - the term 'scanning' itself was reported by several providers to be a perceived as a loaded term, and in several cases they actively avoided using it. Multiple companies told us of experiences with customers that hearing 'scanning' immediately raised concerns, with them being asked if that included SQL injections. Whilst anecdotal, the fact this very specific jump to SQLi was reported from independent interviews does support the view that 'scanning' is a term that can be interpreted as risky. Some companies are opting instead for words like 'measurement', 'analysis' and 'crawling' in place of scanning.

Fingerprinting – another term used frequently by providers. In technical terms this is usually explicitly about the process of using rules/patterns/fingerprints to identify technologies and services running on the organisation's assets. However several providers used it – particularly with less technical audiences – to describe the overall EASM activity of scanning an attack surface.

Language to describe intrusion

Passive – this term was used by some providers to describe the fact that scanning was unintrusive. The NCSC typically considers passive[5] to mean not interacting directly with the asset at all, but this is not how providers used it. In all cases where scanning was described as 'passive', some level of interaction was occurring either by the provider or a scanning data supplier (eg an internet-wide scanner). In all cases, the intrusion level of the scanning was low, often of the equivalence of a normal user using the services (for example browsing a website). Passive was generally used to mean that it wouldn't negatively affect the services, or that no unauthorised access would take place. We observed 'passive' to be an unhelpful term, as it lacks definition, and was used to mean different things by different providers.

Public data – several providers discussed emphasising to customers that all the data they capture is publicly available. If they can collect it, so can anyone else. "*Anything you shouldn't be showing us, we shouldn't be able to see*". From conversations with providers and our own first-hand observations, we observed that many customers find what is public alarming, in some cases raising concerns about services (such as some internet-wide scanners) exposing this information to the public. There may be a space here for the NCSC to provide education and thought leadership about what is public, and if/why open access to that information is in the interests of defenders.

Same as a user – there was no specific term for this, but many providers told us how they describe their scans as being equivalent to a "*normal user, doing normal things*" such as browsing web pages, or basic

[5] https://www.ncsc.gov.uk/guidance/asset-management#section_6

interaction with services. This was also used in the context of traffic volume, stating that a single user could easily create the same volume of traffic as their scans.

Payload testing – variations of this term ('payload scanning', 'payload-based testing', 'functional exploitation', etc) were used by multiple providers to describe a type of vulnerability scanning whereby non-malicious exploit payloads are targeted at known vulnerabilities to check if they are exploitable on the organisation's system. Providers commented that "*you really need to be doing payload scanning to have any accuracy with vulnerability scans*". Some providers commented on the challenges of describing to customers why this increased risk is worthwhile.

Conclusion – A wide variety of loosely defined language is being used to describe scanning activities, sometimes with conflicting meanings. Providers are avoiding using accurate technical terms in favour of words that raise less concern from customers. There is no common framework for describing scanning activities or levels of intrusion.

Conclusion – Customers are routinely raising concerns about potential impact of EASM scanning activity, overlooking the existing ever-present risk that any online asset can be scanned by anyone at any time.

The future of EASM

Provider views

Discussing the future of EASM and the market in the next five years with providers, there were varying predictions, which reinforces the individuality of many EASM providers and their specialised focus as well as the customers they work with and their cyber security maturity. There is no one answer, and one size does and will not fit all when it comes to EASM solutions.

Whilst one provider explained that "*the hype cycle is over, everyone knows what the acronym means*," another highlighted "*a lot of companies would benefit [from EASM] but don't know if they realise that*". Many of the organisations we worked with through our experiments did not know what EASM stood for or what it meant for them. There is still a need for educating organisations across the public and private sectors.

There is a concern that current EASM practices are overwhelming customers, with some providers using the "*power of marketing*" and focusing on "*the hype*" rather than on "*what people actually need*." Where some offer risk scoring, others refer to this as "*snake oil*" for organisations that can often distract and cause "*unnecessary stress and drama*". There is a fear all of this will lead to people disengaging from EASM which is "*an important point of cyber security*".

A theme is clearly emerging for understanding customer needs and encouraging them to see the bigger picture and understand that EASM is just one piece of their cyber security puzzle. Some providers have a vision of the industry "*pulling everything in from the jigsaw to give that one view*"; they understand that "*EASM pairs well with other things*," and see the value in focusing on what they do best and collaborating with other providers in the industry to provide that fuller picture to their customers – "*you can't be best at everything.*"

Conclusion – Providers will continue to offer their take on EASM solutions to meet the varied and sometimes unique security needs of organisations – customers will need a way to understand the right solution(s) for them.

Customer organisation thoughts

Of the 27 organisations participating in this experiment, 36% had no experience of using an EASM solution and after completing the trials, only 71% would choose to use one in the future. Of those that were unsure, cost played a big part in their decision as most organisations have limited budget and they need to confidently understand the value of a solution before they invest in it. Maturity, experience and ability to manage the tools play a part in this decision-making process.

Those choosing to use an EASM solution in the future see it as an important tool to help them "*develop a fuller threat picture*". Some with more experience, talked about using it to "*have visibility beyond our direct domain and allow us to have an eye on our partners*" whilst others are looking for the "*reassurance that we are working correctly and not accidentally or on purpose exposing our resources.*" Others who work in IT roles but do not see themselves as 'cyber security experts', highlighted the value of support the solution brings as they "*rely on the systems, experience and knowledge of others and this is one important tool in our arsenal against the continuous cyber threats we experience*."

When choosing an EASM solution in the future, our participating organisations valued ease of use and integrations as well as features specific to their requirements. Cost, feedback, features and demonstrations are key factors in their decision-making process. The experiment itself was invaluable to most in advancing their knowledge of EASM solutions and informing future decisions - "*this trial has reinforced the importance of EASM in our cybersecurity strategy, particularly in providing assurance to the board regarding our attack surface management*." Others added "*it's opened our eyes to the benefits of this kind of solution*", and "*this trial has made a compelling case that we need to consider an EASM.*" There is great value in hands-on experience.

Conclusion – Organisations' ASM needs will vary with a range of internal factors including their cyber security expertise and organisational structure.

Conclusion – Cost is a crucial factor for organisations when choosing tools and solutions. They need confidence that they are spending their budget on the right thing for them.

NCSC.GOV.UK @NCSC @CYBERHQ @CYBERHQ National Cyber Security Centre