WHITE PAPER

Minimizing Your Digital Footprint: The Importance of External Attack Surface Management (EASA)

Secura
A BUREAU VERITAS COMPANY

Secura's External Attack Surface Assessment (EASA) service

The attack surface of organizations all over the world is expanding. The interconnectivity of organizations, the use of smart devices, intelligent systems, social media and SaaS-services: the ways in which an attacker can potentially access your organization have grown drastically. This means that simple vulnerability scans on IP ranges are no longer enough to detect the dangers coming your way. You need a wider scope. According to Gartner, External Attack Surface magagement is one of the new ways to protect your organization against growing threats.

Cybersecurity checks

Secura is proud to be one of the first companies to offer you an External Attack Surface Assessment (EASA). Our EASA combines four of the most important cybersecurity checks into one assessment. This means we can give you a full view of your susceptibility to external attacks like ransomware or databreaches. These four checks are:

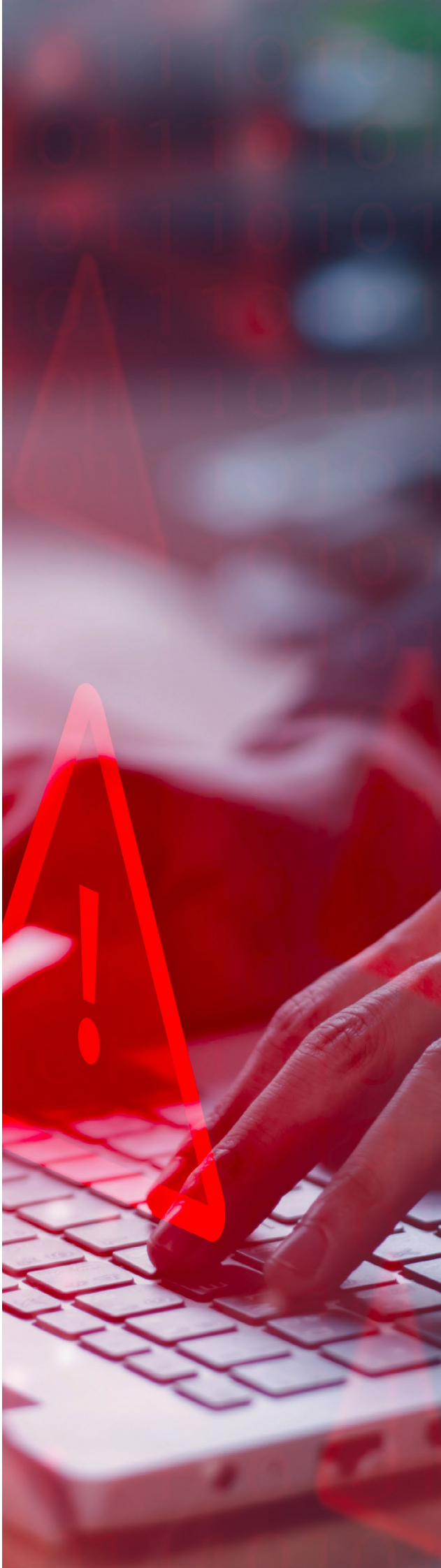
1. Discovery. The chances are high that you do not have a full view of your internet-facing assets. We perform far-reaching asset discovery, by querying high-quality 3rd party data sources and performing extensive scans.
2. Credentials. Your users' passwords are probably already out there on the internet, or being sold on the dark web. We check if this is indeed the case, for instance by scraping dark web marketplaces or searching repositories of password breaches.
3. Exposures. Previous data breaches, management interfaces, leaks or code and data repositories with sensitive information can often be a source for initial access into your network. We check whether you have been breached or exposed.
4. Technical vulnerabilities. We perform wide-reaching vulnerability scans. Things we are on the lookout for include: missing patches and misconfigurations. Of course we also scan the assets you didn't know you had.

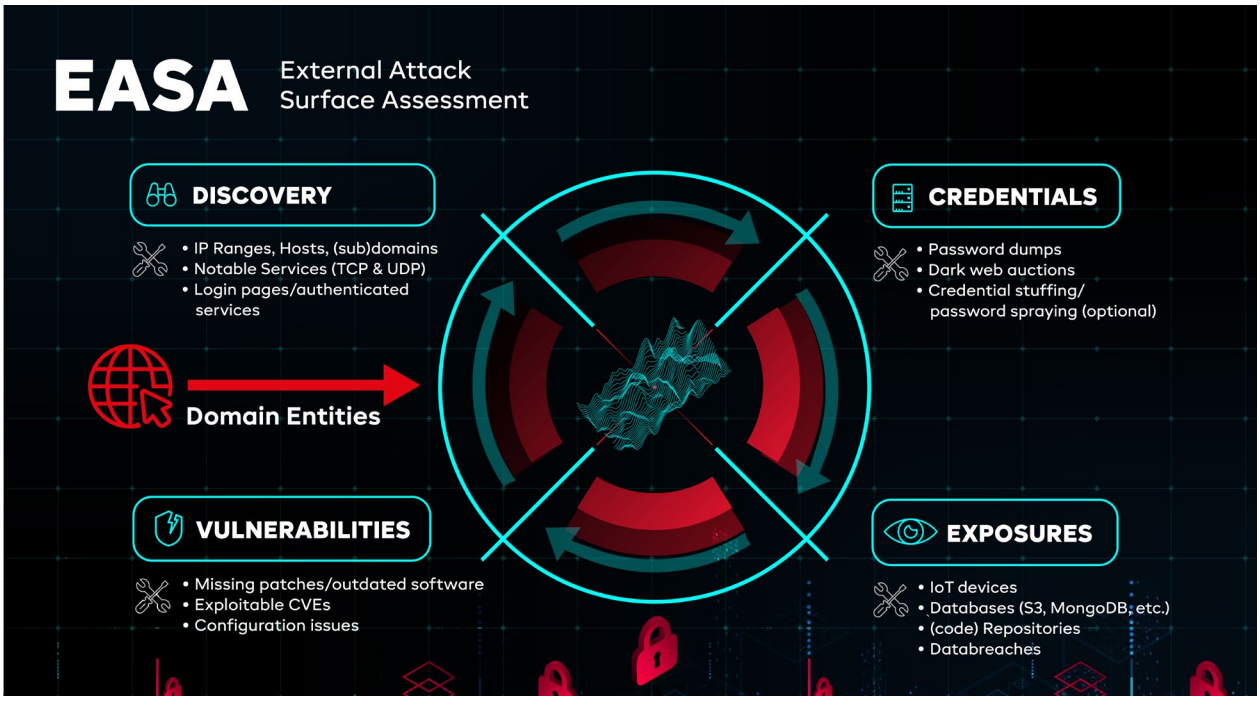
Table of Contents

Goal and approach of an EASA

The goal of an EASA is to **identify relevant vulnerabilities and exposures** that can get you hacked and to give you recommendations for remediation. EASA prioritises any weaknesses and information that is part of actual threat actors' Tactics, Techniques and Procedures (TTP's). The findings we report are concrete and actionable, mapped to Mitre ATT&CK. We prioritize exploitability over technicalities and minor configuration issues. An EASA does not aim to be a full pentest or Open Source Intelligence (OSINT) reporting service, nor does it (cl)aim to identify *all* weaknesses.

This means that technical vulnerabilities that are less relevant for attackers and that do not pose a realistic cybersecurity risk, will not be prioritized in our reporting. Examples of such findings are: SSL/TLS cipher strengths, version numbers in banners, DNS redundancy, ASN routing redundancy or CSP headers in websites. An exposed RDP service is much more likely to be exploited than any of the topics mentioned above. We think it is more important to prioritize the things that can actually get you hacked.





A deeper look at EASA

So what do you get when we perform an EASA for you? Let's look at the four pillars of our EASA in depth:

1. DISCOVERY: ENUMERATING AND OSINTING ENDPOINTS

The starting point for an EASA is not limited to just a list of hosts or IP ranges. Rather, the starting point is one or more domains or subdomain names (secura.com, subdomain.secura.com, et cetera) or entity names (Secura B.V.).

A selection of tools and 3rd-party datasets – such as whois registries, certificate transparency logs, Shodan, Censys and others – serve as a first entry point for endpoint enumeration. These tools and datasets provide a list of assets; often even assets that you may not beaware you had. Additionally, a screenshotting tool helps us to visually enumerate applications on discovered assets.We can later manually triage these for administrative access possibilities.

Because these tools will include various false-positives (in the sense that they will attribute certain assets incorrectly to a customer or domain) and invasive scans cannot be run on non-customer assets, we need you to help us validate all enumerated assets if there is reason to doubt any of these assets.

2. CREDENTIALS: CHECKING PASSWORD DUMPS AND DARKWEB

Over time, millions of accounts have been breached and their passwords have been cracked, including accounts of users that re-use passwords. Or, password stealers on infected endpoints will provide passwords or WebVPN session cookies that are sold on the dark web for initial access. (This is why multi-factor authentication is so important on any internet-facing service, but that is another story)

In this phase of the EASA we will check such data dumps and scrape dark web marketplaces for credentials and endpoint compromises. We will then report on the likelihood of credential stuffing being successful, and if any credential or access has been sold recently. If we know which accounts have been compromised, we will tell you of course. We can even interact with the marketplace – via a proxy party – to obtain the credential or unauthorized access. That way they can be deactivated.

Finally, if you authorize us, we can actually perform a password spraying or credential stuffing attack. That way we can identify weak accounts on login pages in the same way attackers do. Because there are risks attached to this – for instance: account lockouts or excessive logging – we do not perform this test unless you specifically ask us to.

3. IDENTIFYING EXPOSURES AND BREACHES

Have you already been breached? Which part of your organization is exposed? This is what we check during phase 3 of an EASA. To do this we use scrapers, tools and external Threat Intel providers. Things we will try to identify include: data dumps being auctioned on the darkweb, leaked keys and sensitive information in github, pastebin, open Amazon S3 buckets or mongoDB instances.

If any Indicators of Compromise (IoC's) pop up in our feeds that are linked to your assets, we will inform you immediately. We pay close attention to exposed management interfaces, because they can provide an attacker with a privileged way into your systems. The same goes for IoT devices that are exposed and potentially accessible. In the report, we will advise you how to deal with these breaches and exposures.

4. ASSESSING VULNERABILITIES

Finally, the last pillar of an EASA is a classic vulnerability analysis, but with a twist: we prioritise vulnerabilities that can actually get you hacked.

Examples of key things we will be looking for here are:

- Exposed management interfaces (such as RDP, SSH, web UIs on high ports)
- Unencrypted services (such as FTP and HTTP)
- High risk CVEs and known vulnerabilities on any service
- Misconfigurations in services

We use various industry-standard vulnerability scanners, such as Nessus and 'nuclei' for discovering and reporting on vulnerabilities and exposures. It is important to note that we do not test for in-depth application-level vulnerabilities. If you want your applications tested, we offer a full Vulnerability Analysis and Penetration Testing (VA/PT) service here <LINK> that covers all in-depth testing requirements you might have.

Reporting

The output of an EASA is a written report. It includes a management summary, recommendations for remediation, and technical chapters on each of the four pillars of the EASA. The actionable recommendations will allow you to reduce your risk immediately. The individual chapters will provide the details of what we found, where, and what the consequences could be. Obviously, if we find any high-risk or critical findings during the assessment, we will immediately contact you.

We will also include a heatmap and an infographic in the reports to enable you to take a high-level look at how you're doing.

Why Secura?

There are many (new) companies doing External Attack Surface Management or Monitoring. What sets Secura apart from the others?

Personal approach

Most companies offering EASA's are Software as a Service (SaaS)-services. Secura always makes sure you can contact actual human security specialists. Any findings are also validated and analysed by human specialists.

In-depth testing

Most EASA services don't actually test for real vulnerabilities such as CVEs or configuration vulnerabilities. They are quite non-intrusive. There is a good reason for this, because being intrusive requires permissions and indemnifications. If you are operating a global SaaS-service, you need to have a very low entry barrier. Onboarding a new customer should be as simple as paying for the service and proving you own the top level domain. This precludes any invasive attacks/tests.

In Secura's EASA however, onboarding will be a much more interactive process. We will ask for all necessary contracts, permissions and indemnifications, so we can do more invasive vulnerability scans on discovered assets (after your confirmation of course). Being able to perform real vulnerability scans as part of our attack surface assessment services is an important distinguishing factor.

As complete as possible

Many EASA's are not very accurate or complete. Most do basic asset discovery by means of ping scans, DNS queries or reverse IP lookups. Only very few go further and incorporate more obscure but powerful tools such as Certificate Transparency Logs or 3rd-party datasets – such as Shodan or Censys. Combining all these techniquesmeans we can find as many assets as possible. Again, a distinguishing factor of Secura's service.

Additionally, the findings of most other services do not cover as wide a range of aspects as we as security professionals would like to see. Some cover dark market exposures and other Cyber Threat Intelligence (CTI), but will not scan the actual assets. Others do scan assets but don't look at password breaches. Combining as many sensible sources as we can makes our service more complete than other services.

Making sure you know the *actual* risks

Finally, and quite importantly, the issue of false positives and irrelevant risk ratings is still very much a problem in many services. Trivial SSL/TLS vulnerabilities get blown up to high-risk findings (one even scores TLS-1.0 support as a 'critical risk', despite there being no real-life case ever where this was exploited by a threat actor). On the other hand, an open RDP port is still sometimes just included as an informational item in a long list, even though there are many cases in which the exposure of RDP was exploited and led to ransomware attacks.

Well-known and industry-leading security scoring services further condense the findings into a dashboard or even a single score. And of course results usually can be fitted into a user interface. However, we feel that trying to provide a simple presentation usually fails to address the fact that cybersecurity is complex and often cannot be expressed in a single numerical score.

We think that providing insight into the actual risks and exploitable weaknesses is much more valuable to you than providing a simple dashboard or score. This is why we try to bring down the level of false positives and increase the relevance of the risk ratings.

Conclusion

External Attack Surface Assessments are the logical extension and evolution of what we used to call a 'Black-box external infrastructure vulnerability assesssment'. There are many good reasons why you need to stay in control of your attack surface, and that includes aspects that were not included previously, such as password breaches, exposures and dark markets. Secura wraps this up into one neat service that allows you visibility of a lot of surface detail. Please watch this space, because Secura will be introducing a managed (continuous) service based on EASA in the 2nd half of 2023!

Contact us today at info@secura.com or visit secura.com for more information.

SUBSCRIBE

TO OUR NEWSLETTER

About Secura

Secura is a leading expert in digital security. We help our customers- from government and healthcare to finance and industry- to raise their cyber resilience. You can expect high quality security advice, testing, training and certification services from our experts. We believe in an integrated approach to cybersecurity: people, process and technology are equally important. Since 2021, Secura is part of the international Bureau Veritas Group.

Keep updated with the latest insights on digital security and subscribe to our periodical newsletter.

Follow us on:

Secura
A BUREAU VERITAS COMPANY

BUREAU VERITAS
Shaping a World of Trust