

BUREAU
VERITAS

A BUREAU VERITAS COMPANY

External Attack Surface Assessment

Criminal hackers are constantly trying to access your network. The External Attack Surface Assessment (EASA) helps you find your weak spots, so you can take quick action to fix them and deter attackers.

An External Attack Surface Assessment gives you:



Insight into threats

How can an attacker harm you? We check this with scans, Cyber Threat Intelligence and realistic testing.



Understanding of risks

Chances are high you have shadow IT in your organization. This assessment shows you the risks of this.



Actions you can take

Using the results of this assessment, you can take quick action to protect your attack surface.

Why the External Attack Surface Assessment?

Criminal hackers, such as ransomware groups, use anything they can find to attack you, from hacked passwords to vulnerabilities in applications. Do you know which sensitive information is available about your organization to attackers online? Or which internet facing assets your organization has?

An **External Attack Surface Assessment** proactively scans for weaknesses, exposures and vulnerabilities on the perimeter of your organization, combining as many sources as possible: from software repositories to dark web marketplaces. This way, you can take action before criminals can use this information against you.

How the assessment works



1. Discovery

Which internet-facing assets do you have? We start by scanning and mapping these, using one or more domain names or entity names as the starting point.



2. Exposures

You can then expect a scan of the identified assets and public repositories to check for any exposures and data leaks. This includes software repositories, cloud storage and databases.



3. Credentials

It is then time to combine these discovered assets with up-to-date Cyber Threat Intelligence (CTI), for instance credential dumps and dark web marketplaces. We also perform password spraying, to find out if we can access your systems this way.



4. Vulnerabilities

Your identified assets are scanned for technical vulnerabilities and misconfigurations. Few external attack surface providers test discovered assets as thoroughly: you now have a complete picture.

About Secura / Bureau Veritas

Secura is a leading cybersecurity company. We help customers all over Europe to raise their cyber resilience. Our customers range from government and healthcare to finance and industry. We offer technical services, such as vulnerability assessments, penetration testing and red teaming, but also provide audits, forensic services and awareness training.

Secura is a Bureau Veritas company. Bureau Veritas (BV) is a publicly listed company specialized in testing, inspection and certification. BV was founded in 1828, has over 80.000 employees and is active in 140 countries.



Example case | Attack Surface Assessment



Which problem did the customer have?

One Dutch municipality wanted to gain more insight into which of their systems were connected to the internet. They wanted to experience more control.



Result

During the External Attack Surface Assessment, we determined that a system used for management appeared to have been hacked and that login credentials for this system were being sold on the dark web. Because we knew which system had been compromised, this municipality was able to take quick action.



BUREAU
VERITAS

Interested?

Contact us today to start raising your cyber resilience.



info@secura.com



+31 (0) 88 888 3100



secura.com