Secura
A BUREAU VERITAS COMPANY

External Attack Surface Assessment

Are you aware of the data leaks and passwords from your organization that are out there on the internet or dark web? Do you know what legacy applications and IoT devices are connected to the internet? Pay attention, because these exposed assets may pose a threat to your digital security.

What is an External Attack Surface Assessment?

External Attack Surface Assessment (EASA) is the process of **discovering and mitigating vulnerabilities in systems that are connected to the internet**. This includes assets like websites, management interfaces, IoT devices, web applications, payment gateways and cloud services.

With EASA you **improve your cyber resilience and proactively reduce the risk of cyber attacks** by scanning for weaknesses, exposures and vulnerabilities on the perimeter of your organization and beyond.

You'd Be Surprised

Many companies are surprised to discover what can be found about them from sources on the internet. Often we find forgotten, hard-coded passwords in repositories such as Github, or sensitive information in Amazon S3 buckets. Or we notice the use of unsecured APIs or exposed databases without proper authentication. All those exposures and sensitive information are a **treasure trove for attackers** seeking to find a hole in your network defense. This is where performing an External Attack Surface Assessment can help you increase your cyber resilience.

Why Secura?

With over 20 years of experience in offensive security, our customers value us for our experience and knowledge. Choosing Secura for your Attack Surface Assessments has the following additional benefits:

- **Driven by humans**, not simply a SaaS-service
- Tests for **actual vulnerabilities** and not superficial 'potential' vulnerabilities
- Accurate and **comprehensive asset discovery** and **exposure identification**
- No false positives to sift through, only **actionable recommendations**
- **Integration of CTI and dark web activities** such as botnet activitity
- **Relevant risk rating** based on real-world exploitability.

Secura
A BUREAU VERITAS COMPANY

Four Areas of Focus in Attack Surface Assessment

Within the External Attack Surface Assessment (EASA), Secura investigates four main areas:

1 Discovery

Discover what assets in your organization are accessible by external parties through the internet. We will assess the risks associated with those assets.

2 Credentials

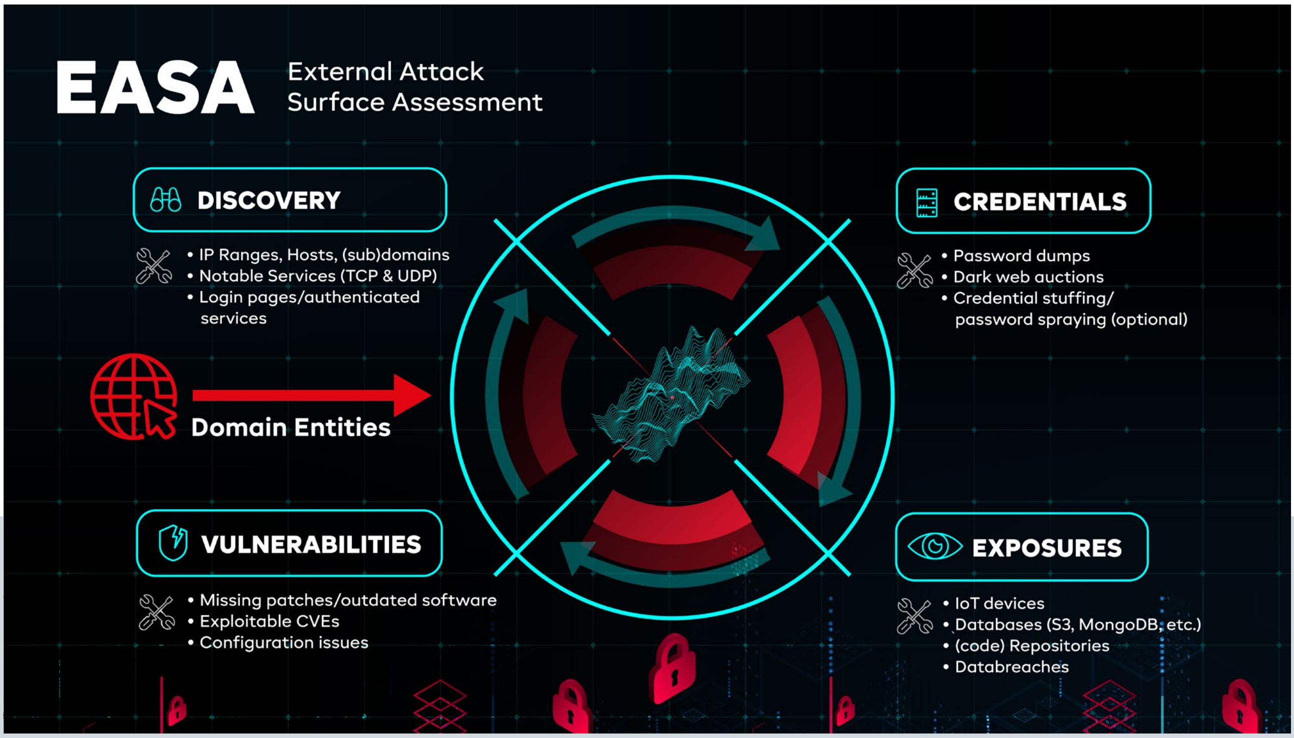
Search on the internet and on the dark web what credentials are dumped, traded or for sale for your organization. How were those usernames and passwords obtained? You might have to disable specific endpoints or users.

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.



EASA External Attack Surface Assessment

DISCOVERY
- IP Ranges, Hosts, (sub)domains
- Notable Services (TCP & UDP)
- Login pages/authenticated services

Domain Entities

CREDENTIALS
- Password dumps
- Dark web auctions
- Credential stuffing/ password spraying (optional)

VULNERABILITIES
- Missing patches/outdated software
- Exploitable CVEs
- Configuration issues

EXPOSURES
- IoT devices
- Databases (S3, MongoDB, etc.)
- (code) Repositories
- Databreaches

Secura
A BUREAU VERITAS COMPANY

Interested?

Contact us today:

Follow us:

☎ +31 88 888 31 00

✉ info@secura.com

secura.com

BUREAU VERITAS 1828

Shaping a World of Trust