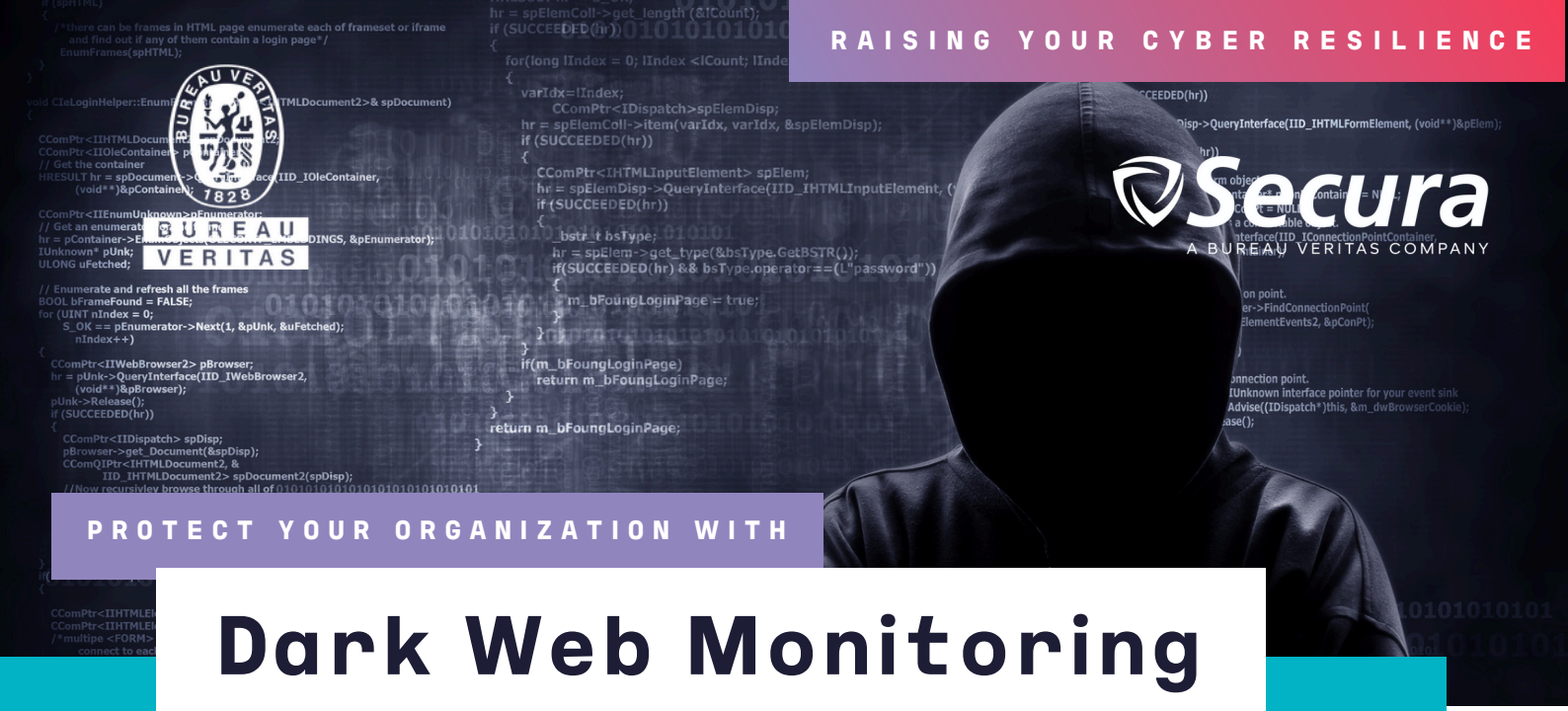

PROTECT YOUR ORGANIZATION WITH

Dark Web Monitoring

Do you know if potential attackers can find stolen credentials from your organization on the dark web? We can monitor this for you. This is important, because stolen credentials are the main cause of security breaches. Find out before attackers use this information against you.

Dark Web Monitoring gives you:

Hard-to-get information

Valuable information from the dark web is hard to come by. Our unique information position can help you.

Actions to protect yourself

Which accounts and systems are affected? We can help you identify these and advise you on actions.

An ethical partner

Navigating illegal marketplaces comes with dilemmas. Our experts follow the most ethical course.

Why choose Dark Web Monitoring?

By scanning the dark web, or illegal online marketplaces, we can discover if criminals are selling or trading in access to your assets. This means you can take immediate protective measures, before this information is used against you. We specifically search for credentials stolen from compromised systems. This is important, because cybercriminals can use stolen credentials or compromised systems as a gateway to access the rest of your network. An infected system is often a precursor to a ransomware attack.

Dark Web Monitoring serves as the last line of defense - if attackers have managed to break through your other security measures, this service can give your valuable information to stop them just in time.

How Dark Web Monitoring works

1. Scope and baseline

Which (sub)domains do you want to monitor? The first step is to give you a baseline of information that is already available about your organization on the dark web. On that basis we will define the scope for future alerts.

2. Daily monitoring

We monitor the dark web daily for stolen credentials for your assets and compromised endpoints, to make sure that we stay up-to-date on intelligence.

3. Validation

Not all information is equally important, relevant or urgent. Our experts validate any new information that the monitoring shows.

4. Notifications and recommendations

If there is a serious threat, you receive an immediate notification. You receive insight into which accounts and systems have been compromised. You can expect us to help you determine the best course of action, so that you can protect your organization from potential attackers.

Why Dark Web Monitoring is important

Dark Web Monitoring can prevent a lot of damage. Recently credentials of a large US tech healthcare company were stolen by a credential stealer and bought by the BlackCat ransomware group. This group used these credentials to gain remote access, move laterally and exfiltrate sensitive medical data on a substantial portion of people in America.

The hack disrupted healthcare payments in the USA for a month. The company paid $22 million to recover access to data and systems and to prevent data from being published. But the company expects the hack to cost up to $1.6 billion. All because the credentials of one employee were sold on the dark web.

Interested?

Contact us today to start raising your cyber resilience.

info@secura.com
+31 (0) 88 888 3100
secura.com

Secura
A BUREAU VERITAS COMPANY

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.