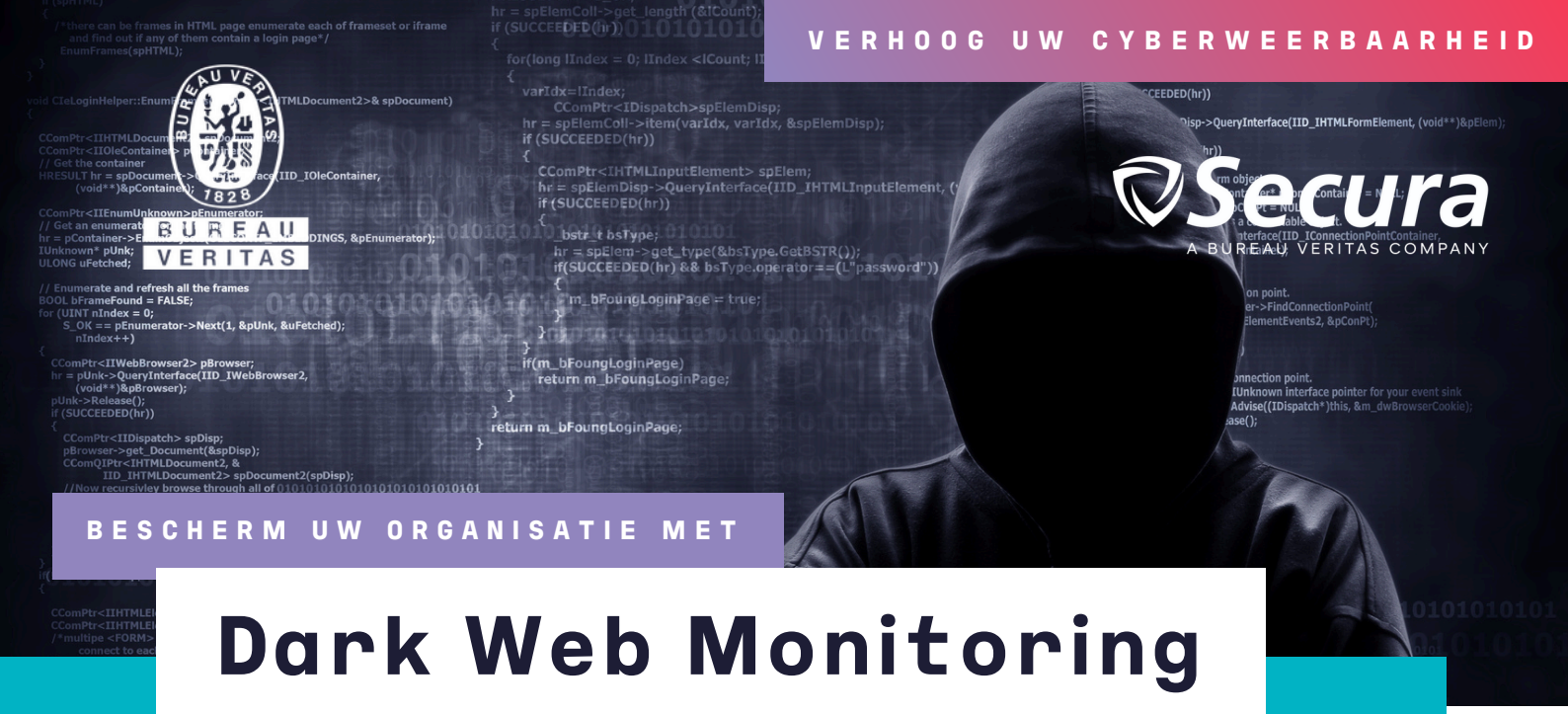

BESCHERM UW ORGANISATIE MET

Dark Web Monitoring

Weet u of potentiële aanvallers gestolen inloggegevens van uw organisatie kunnen vinden op het dark web? Wij kunnen dit voor u monitoren. Dit is belangrijk, want gestolen inloggegevens zijn de belangrijkste oorzaak van beveiligingslekken.

Dark Web Monitoring geeft u:

Moeilijk verkrijgbare info

Waardevolle informatie is op het dark lastig te krijgen. Onze unieke informatiepositie kan u helpen.

Actie om uzelf te beschermen

Welke accounts en systemen zijn getroffen? Wij helpen u dit te bepalen en adviseren over maatregelen.

Een ethische partner

Illegale marktplaatsen brengen dilemma's met zich mee. Onze experts kiezen de meest ethische weg.

Waarom Dark Web Monitoring?

Door het dark web of illegale online marktplaatsen te scannen, zien we of criminelen toegang tot uw assets verkopen of verhandelen. Dit betekent dat u direct maatregelen kunt nemen voordat deze informatie tegen u wordt gebruikt. We zoeken specifiek naar inloggegevens die zijn gestolen van gecompromitteerde systemen. Dit is belangrijk, want cybercriminelen kunnen gestolen inloggegevens of gecompromitteerde systemen gebruiken als toegangspoort tot de rest van uw netwerk. Een geïnfecteerd systeem is vaak een voorbode van een ransomware-aanval.
Dark Web Monitoring dient als laatste verdedigingslinie - als aanvallers erin zijn geslaagd om door uw andere beveiligingsmaatregelen heen te breken, kan deze dienst uw waardevolle informatie geven om ze net op tijd tegen te houden.

Hoe Dark Web Monitoring werkt

1. Scope en baseline

Welke (sub)domeinen wilt u monitoren? De eerste stap is om een baseline op te stellen van informatie die al beschikbaar is over uw organisatie op het dark web. Op basis hiervan bepalen we de scope voor toekomstige alerts.

2. Dagelijkse monitoring

Wij monitoren het dark web dagelijks op gestolen inloggegevens voor uw assets en gecompromitteerde systemen, zodat we op de hoogte blijven van de laatste informatie.

3. Validatie

Niet alle informatie is even belangrijk of urgent. Onze experts valideren alle nieuwe informatie die de monitoring laat zien.

4. Notificaties en aanbevelingen

Als er sprake is van een ernstige bedreiging, ontvangt u onmiddellijk een melding. We maken inzichtelijk welke accounts en systemen gecompromitteerd zijn. U kunt hulp verwachten bij het bepalen van de beste aanpak, zodat u uw organisatie kunt beschermen tegen potentiële aanvallers.

Secura
A BUREAU VERITAS COMPANY

Over Secura / Bureau Veritas

Secura is een toonaangevend cybersecuritybedrijf. Ons doel is om uw cyberweerbaarheid te vergroten. Onze klanten variëren van overheid en zorg tot financiën en industrie. Secura biedt technische diensten aan, zoals vulnerability assessments, penetratietesten en red teaming. We bieden ook audits, forensische diensten en awarenesstrainingen aan.

Secura is onderdeel van Bureau Veritas (BV), een beurs-genoteerde onderneming die gespecialiseerd is in testen, inspecteren en certificeren. BV is opgericht in 1828, heeft ruim 80.000 medewerkers en is actief in 140 landen.

Zo belangrijk is Dark Web Monitoring

Dark Web Monitoring kan veel schade voorkomen. Onlangs werden inloggegevens van een groot Amerikaans techbedrijf in de gezondheidszorg gestolen door een ‘credential stealer’ en gekocht door de BlackCat ransomware-groep. Deze groep gebruikte de inloggegevens om gevoelige medische gegevens van een groot deel van de Amerikaanse bevolking te exfiltreren.

Het bedrijf betaalde 22 miljoen dollar om toegang tot data en systemen te herstellen en om publicatie van de data. Maar het bedrijf verwacht dat de hack tot 1,6 miljard dollar zal kosten. En dat allemaal omdat de inloggegevens van één werknemer werden verkocht op het dark web..

BUREAU VERITAS 1828

Meer weten?

Neem contact met ons op om uw cyberweerbaarheid te verhogen.

info@secura.com

+31 (0) 88 888 3100

secura.com