

Leaked Credentials Monitoring

Secutec SecureSIGHT



Prevent now, secure tomorrow

Versterk uw verdediging met leaked credentials intelligence

Leaked credentials is de term die elke ongeoorloofde vrijgave van **persoonlijke of organisatielogins** omvat, inclusief gebruikersnamen, wachtwoorden en persoonlijk identificeerbare gegevens (PID). Ze hebben betrekking op verschillende soorten accounts, zoals e-mail, sociale media, bankieren of bedrijfsnetwerken en worden veroorzaakt door externe database-inbreuken, **password stealers** die niet zijn opgemerkt door traditionele antivirus systemen, phishing, hacks of nalatigheid van gebruikers.

Leaked credentials vormen een grote bedreiging

In 2022 kwam bijna DE HELFT van alle gecompromitteerde gegevens die werden gevonden op het darknet, voort uit apparaten die geïnfecteerd waren met malware¹. **Leaked credentials dienen voor cybercriminelen als de belangrijkste toegangspoort tot bedrijfsnetwerken.** Met deze geldige wachtwoorden wordt ongeoorloofde toegang een aanzienlijk risico, waarbij een sleutel wordt geboden om beveiligingsmaatregelen te omzeilen en mogelijk persoonlijke, financiële of organisatorische gegevens in gevaar te brengen.

Hoe SecureSIGHT het risico beperkt

Nu cyberbedreigingen steeds geavanceerder worden, is het onvoldoende om alleen op traditionele beveiligingsprotocollen te vertrouwen. Hoewel standaard veiligheidsmaatregelen en Multi-Factor Authenticatie (MFA) cruciale eerste stappen zijn, zijn organisaties nog steeds kwetsbaar voor onbeheersbare factoren zoals zwakke wachtwoorden en nalatig gedrag van medewerkers. De module Leaked Credentials Monitoring van Secutec SecureSIGHT biedt een **proactieve laag voor uw beveiligingsinfrastructuur** en biedt inzicht in gecompromitteerde gebruikersnamen en wachtwoorden, waardoor uw bedrijf **in een vroeg stadium kan ingrijpen en extra schade aan uw bedrijfsomgeving kan voorkomen.**



Darknet Search

Wij speuren het darknet af naar geldige gelekte logingegevens die gekoppeld zijn aan uw bedrijf en zijn gebruikers.



Onmiddellijke waarschuwingen

Ontvang geïnterpreteerde waarschuwingen en inzichten in realtime.



Identificatie van gegevens

We categoriseren alle logingegevens en maken onderscheid tussen aanmeldingen van werknemers, klanten, derden en externe websites.



Identificatie van geïnfecteerde hosts

Wij bieden informatie om u te helpen de host te identificeren waarop malware is geïnstalleerd.



Geen IT-infrastructuurwijzigingen

Onze gehoste infrastructuur integreert naadloos met uw bestaande installatie.



Maandelijks rapportage

Ontvang regelmatig (executive) rapporten.



Support

We adviseren u over de beste volgende stappen om de inbreuk op te lossen.



Managed Service of eenmalig rapport

Concentreer u op uw kerntaken terwijl wij de bewaking voor onze rekening nemen.

Benieuwd naar de effectiviteit van onze oplossing?

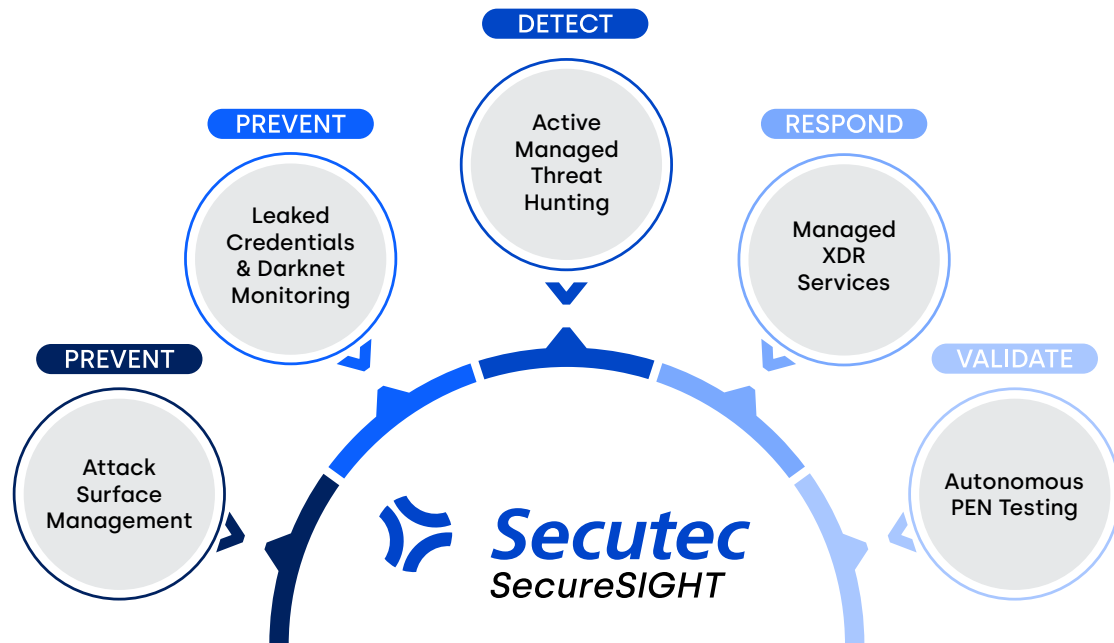
Neem contact met ons op voor een eenmalig monitoringrapport en een demonstratie van alle dashboards en functionaliteiten.

¹ SpyCloud 2023 Annual Identity Exposure Report

Wij bewaken voortdurend uw digitale grenzen

De **managed service** van Secutec SecureSIGHT biedt de meest kostenefficiënte oplossing die de meest cruciale aspecten van de levenscyclus van een cyberaanval bestrijkt door een breed scala aan aanvalsvectoren en indicators of compromise (IOC's) te analyseren. Het **Secutec Security Operations Center (SOC)** van Secutec verzamelt alle gegevens over mogelijke aanvallen, voegt context toe aan meldingen en levert bruikbare gegevens en geïnterpreteerde inzichten.

Secutec SecureSIGHT biedt **5 verschillende modules** die zijn afgestemd op uw specifieke behoeften en gebruik maken van uw bestaande beveiligingsinfrastructuur.



ATTACK SURFACE MANAGEMENT

We identificeren en beheren alle **potentiële kwetsbaarheden en zwakke punten** in de digitale omgeving van uw organisatie die kunnen worden uitgebuit door cyberaanvallers. Het doel is om uw algehele risico te verminderen door het aantal **mogelijke toegangspunten voor aanvallers te minimaliseren** en ervoor te zorgen dat bestaande kwetsbaarheden op de juiste wijze worden geïdentificeerd en geprioriteerd.

LEAKED CREDENTIALS & DARKNET MONITORING

We bieden inzicht in **gecompromitteerde gebruikersnamen en wachtwoorden** uit datalekken, waardoor uw bedrijf proactief accountmisbruik kan voorkomen. Onze waakzame monitoring van het darknet identificeert tekenen van dreigende aanvallen en potentiële datalekken.

ACTIVE MANAGED THREAT HUNTING

We jagen actief op **indicators of compromise (IOC)**. Onze SecureSIGHT-intelligentie blinkt uit in het detecteren van geavanceerde bedreigingen die vaak over het hoofd worden gezien door conventionele systemen, en past zich voortdurend aan aan het steeds veranderende cyberdreigingslandschap, zodat u snel kunt reageren op beveiligingsincidenten.

MANAGED XDR SERVICES

Endpoint- en serverbeveiliging zijn van het grootste belang in het licht van cyberdreigingen. Onze XDRoplossing - **Extended Detection and Response** - biedt 24/7 geavanceerde dreigingsdetectie, realtime zichtbaarheid, snelle incidentrespons, compliance en gebruiksgemak.

AUTONOMOUS PEN TESTING

Om de bestaande **beveiligingsmaatregelen te beoordelen**, proberen we **kwetsbaarheden en zwakke punten** in de doelomgeving uit te buiten. Deze proactieve benadering stelt ons in staat eventuele blinde vlekken te identificeren en uiteindelijk uw algehele veerkracht op het gebied van cyberbeveiliging te verbeteren.