Leaked Credentials & Darknet Monitoring

Secutec
Cyber security intelligence

Secutec SecureSIGHT

Shine a light on the darknet with our 24/7 managed darknet monitoring service

Credential leakage monitoring is a critical cybersecurity practice where we continuously monitor for instances where an organization's usernames and passwords, encompassing both internal employees and third-party entities, have been exposed or compromised. This monitoring is essential for several reasons:

- ✓ Protection against **unauthorized access**
- ✓ Mitigating **account takeover** attacks
- ✓ Protect **customer data and sensitive information**
- ✓ Expose **sleeping accounts**
- ✓ Fulfill industry **compliance** and maintain **trust**
- ✓ Third-party and supply chain **risk monitoring**

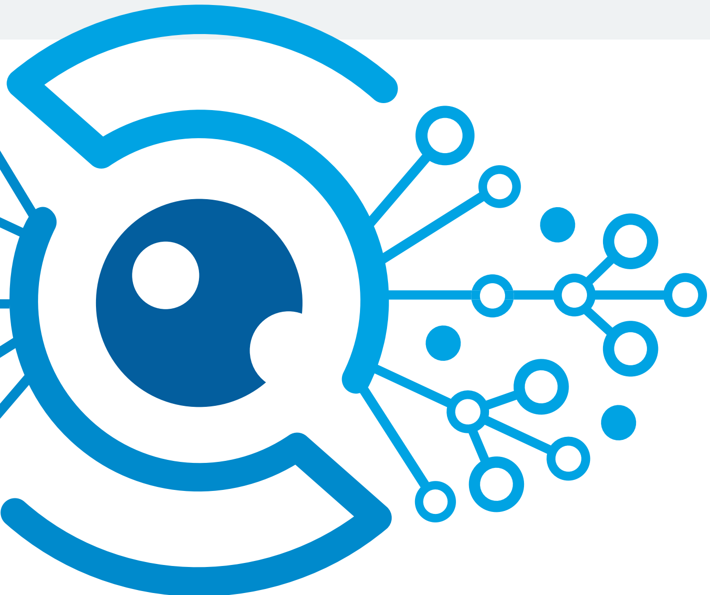
Our **darknet scans** help organizations to protect their sensitive information, maintain compliance, and mitigate the risks associated with credential exposure. It is a **proactive measure to safeguard against emerging threats, unauthorized access and data leaks** in an increasingly interconnected and digital world. Our approach involves **active filtering** through the darknet's vast expanse, seeking out crucial information such as company and domain names, brands, VP's, C-level employee names, specific keywords, and discernible patterns. Our **automated scans** operate around the clock and are supported by an extensive repository of threat intelligence data.

Armed with these insights, you gain a **comprehensive view or your organization's risk profile** allowing you to efficiently prioritize and remediate potential risks quickly.

Did you know that in 2022...

1. 721 million total exposed credentials were recovered from the darknet
2. 22.3 million unique machines were infected with malware
3. 72% of users involved in breaches reused previously exposed passwords

source: SpyCloud 2023_Identity_Exposure_Report



How we protect you

IMMEDIATE ALERTING

When potential credential exposures are detected.

IDENTIFICATION OF INFECTED EMPLOYEES

Receive all information on compromised credentials, the source of the leak and potential impact.

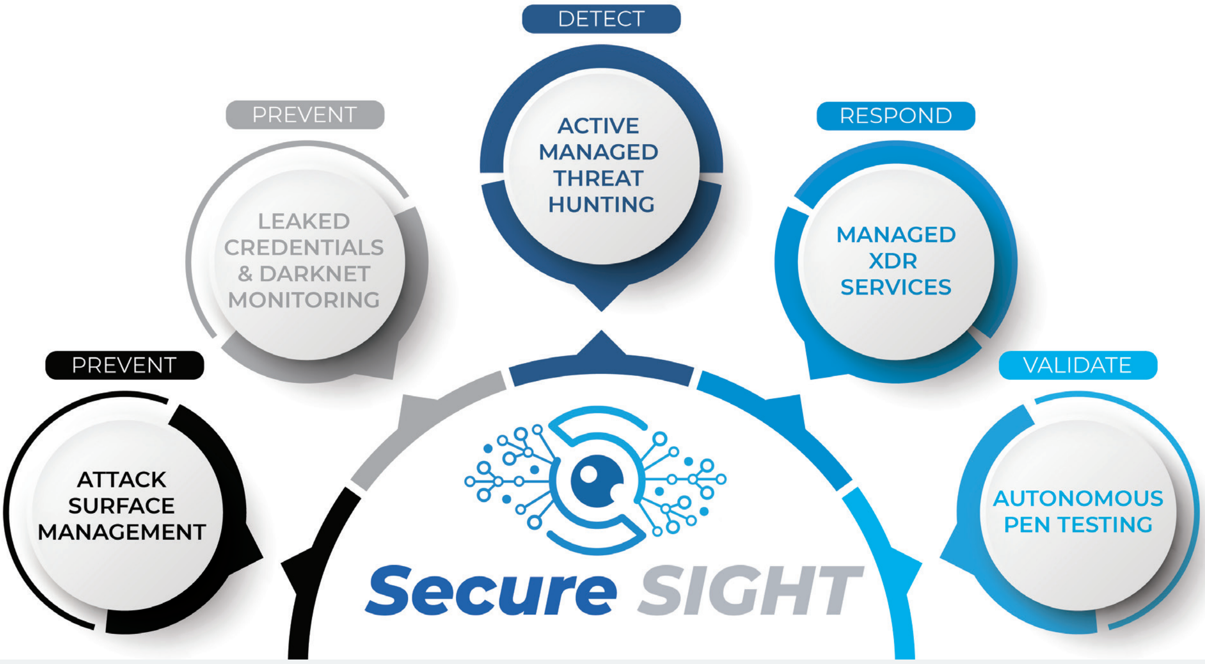
INSTANT REPORTING OF MALICIOUS ACTIVITIES

To prevent breaches and data leaks that can put your organization at risk.

Continuously patrolling your digital perimeter

Secutec SecureSIGHT's **managed service** offers the most cost-efficient solution that covers the most crucial aspects of a cyber attack's life cycle by analyzing a wide range of attack vectors and indicators of compromise. The **Secutec Security Operations Center** (SOC) collects all data about possible attacks, adds context to alerts and provides you with actionable data and interpreted insights.

Leveraging your current security infrastructure, Secutec SecureSIGHT presents **5 different modules** tailored to your specific requirements.


DETECT
ACTIVE MANAGED THREAT HUNTING
PREVENT
LEAKED CREDENTIALS & DARKNET MONITORING
RESPOND
MANAGED XDR SERVICES
PREVENT
ATTACK SURFACE MANAGEMENT
VALIDATE
AUTONOMOUS PEN TESTING
Secure SIGHT

ATTACK SURFACE MANAGEMENT

We identify and manage all **potential vulnerabilities and weaknesses** in your organization's digital environment that could be exploited by cyber attackers. The goal is to reduce your overall risk by **minimizing the number of potential entry points** for attackers and ensuring that vulnerabilities that do exist are properly identified and prioritized.

LEAKED CREDENTIALS & DARKNET MONITORING

We provide visibility into **compromised usernames and passwords** from data breaches, empowering your company to proactively prevent account abuse. Our vigilant monitoring of the darknet identifies signs of impending attacks and potential dataleaks.

ACTIVE MANAGED THREAT HUNTING

We actively hunt for any **Indicators of Compromise (IOC)**. Our SecureSIGHT intelligence excels at detecting advanced threats often overlooked by conventional systems, continuously adjusting to the ever-evolving cyber threat landscape, enabling you to respond rapidly to security incidents.

MANAGED XDR SERVICES

Endpoint and server security is paramount in the face of cyber threats. Our XDR solution - **Extended Detection and Response** - offers round-the-clock advanced threat detection, real-time visibility, rapid incident response, compliance, and ease of use.

AUTONOMOUS PEN TESTING

We attempt to **exploit vulnerabilities and weaknesses** in the target environment to **assess** the existing security measures in place. This proactive approach allows us to identify any blind spots, ultimately enhancing your overall cyber security resilience.

V02-2024