

# Leaked Credentials Monitoring



## Secutec SecureSIGHT

### Empowering your defenses with leaked credentials intelligence

**Leaked credentials** is the name that covers any **unauthorized disclosure of personal or organizational login details**, including usernames, passwords, and personal identifiable data (PID). They relate to various types of accounts, such as email, social media, banking, or corporate networks and are caused by external database breaches, **password stealers** that have not been picked up by traditional anti-virus systems, phishing, hacks, or user negligence.

### Why leaked credentials pose a significant threat

In 2022, nearly HALF of compromised credentials retrieved from the darknet resulted from malware-infected devices<sup>1</sup>. **Leaked credentials serve as the primary gateway for cybercriminals into corporate networks.** With these legitimate passwords, unauthorized access becomes a significant risk, presenting a key to bypass security measures and potentially compromising personal, financial, or organizational data.

### How SecureSIGHT mitigates the risk

As cyber threats grow in sophistication, relying solely on traditional security protocols has become insufficient. While standard safety measures and Multi-Factor Authentication (MFA) are crucial initial steps, organizations are still vulnerable to uncontrollable factors such as weak passwords and negligent employee behavior. Secutec SecureSIGHT's Leaked Credentials Monitoring module offers a **proactive layer to your security infrastructure**, providing visibility into compromised usernames and passwords, **empowering your company to intervene at an early stage** and **avoid additional damage** to your corporate environment.



#### Darknet Search

We scour the darknet for valid leaked credentials associated with your business and its users.



#### No IT Infrastructure Changes

Our hosted infrastructure seamlessly integrates with your existing setup.



#### Instant Alerts

Receive interpreted alerts and insights in real-time.



#### Monthly Reporting

Benefit from regular (executive-level) reports.



#### Credential Identification

We categorize credentials, distinguishing between employee, customer, third party, and external website logins.



#### Support

We can advise on the best next steps to take to resolve the breach.



#### Infected Host Identification

We provide information to help you identify the host on which malware was installed.



#### Managed Service or One-Shot Report

Focus on core tasks while we handle the monitoring.

Curious to witness the effectiveness of our solution?

**Contact us for a one-shot monitoring report and a demonstration of all dashboards and functionalities.**

<sup>1</sup> SpyCloud 2023 Annual Identity Exposure Report

# 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.



## 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.