

Leaked Credentials Monitoring

Secutec SecureSIGHT



Prevent now, secure tomorrow

Stärken Sie Ihre Abwehr mit Leaked Credentials Intelligence

Unter dem Begriff „**Leaked Credentials**“ (durchgesickerte Anmeldedaten) versteht man die unbefugte Offenlegung von **persönlichen oder organisatorischen Anmeldedaten**, einschließlich Benutzernamen, Passwörtern und personenbezogenen Daten (PID). Sie beziehen sich auf verschiedene Arten von Konten, wie E-Mail, soziale Medien, Bankgeschäfte oder Unternehmensnetzwerke, und werden durch externe Datenbankverletzungen, Passwortdiebstahl, der von herkömmlichen Antiviren-Systemen nicht erkannt wurde, Phishing, Hacks oder Fahrlässigkeit der Benutzer verursacht.

Warum Leaked Credentials eine große Gefahr darstellen

Im Jahr 2023 waren über 60 % aller Datenschutzverletzungen malwarebedingt und umfassten 343,78 Millionen gestohlene Zugangsdaten¹. **Leaked credentials dienen Cyberkriminellen als Haupteinfallstor in Unternehmensnetzwerke**. Mit diesen legitimen Passwörtern wird der unbefugte Zugriff zu einem erheblichen Risiko, da sie einen Schlüssel zur Umgehung von Sicherheitsmaßnahmen darstellen und persönliche, finanzielle oder organisatorische Daten gefährden können.

Wie SecureSIGHT das Risiko abmildert

Da die Cyber-Bedrohungen immer raffinierter werden, reicht es nicht mehr aus, sich nur auf herkömmliche Sicherheitsprotokolle zu verlassen. Während Standard-Sicherheitsmaßnahmen und Multi-Faktor-Authentifizierung (MFA) wichtige erste Schritte sind, sind Unternehmen immer noch anfällig für unkontrollierbare Faktoren wie schwache Passwörter und fahrlässiges Mitarbeiterverhalten. Secutec SecureSIGHT's Leaked Credentials Monitoring Modul bietet eine **proaktive Ebene für Ihre Sicherheitsinfrastruktur**, indem es Einblicke in kompromittierte Benutzernamen und Passwörter bietet und Ihr Unternehmen in die Lage versetzt, **in einem frühen Stadium einzugreifen und zusätzliche Schäden an Ihrer Unternehmensumgebung zu vermeiden**.



Darknet Search

Wir durchsuchen das Darknet nach gültigen, durchgesickerten Anmeldedaten, die mit Ihrem Unternehmen und seinen Benutzern



Sofortige Warnungen

Sie erhalten interpretierte Warnmeldungen und Einblicke in Echtzeit.



Identifizierung der Daten

Wir kategorisieren die Anmeldedaten und unterscheiden zwischen Mitarbeiter-, Kunden-, Drittanbieter- und externen Website-Anmeldungen.



Identifizierung infizierter Hosts

Wir stellen Informationen zur Verfügung, die Ihnen helfen, den Host zu identifizieren, auf dem die Malware installiert wurde.



Keine Änderungen der IT-Infrastruktur

Unsere gehostete Infrastruktur fügt sich nahtlos in Ihr bestehendes System ein.



Monatliche Berichterstattung

Profitieren Sie von regelmäßigen Berichten (auf Führungsebene).



Support

Wir können Sie über die besten nächsten Schritte zur Behebung des Verstoßes beraten.



Managed Service oder Einmaliger Bericht

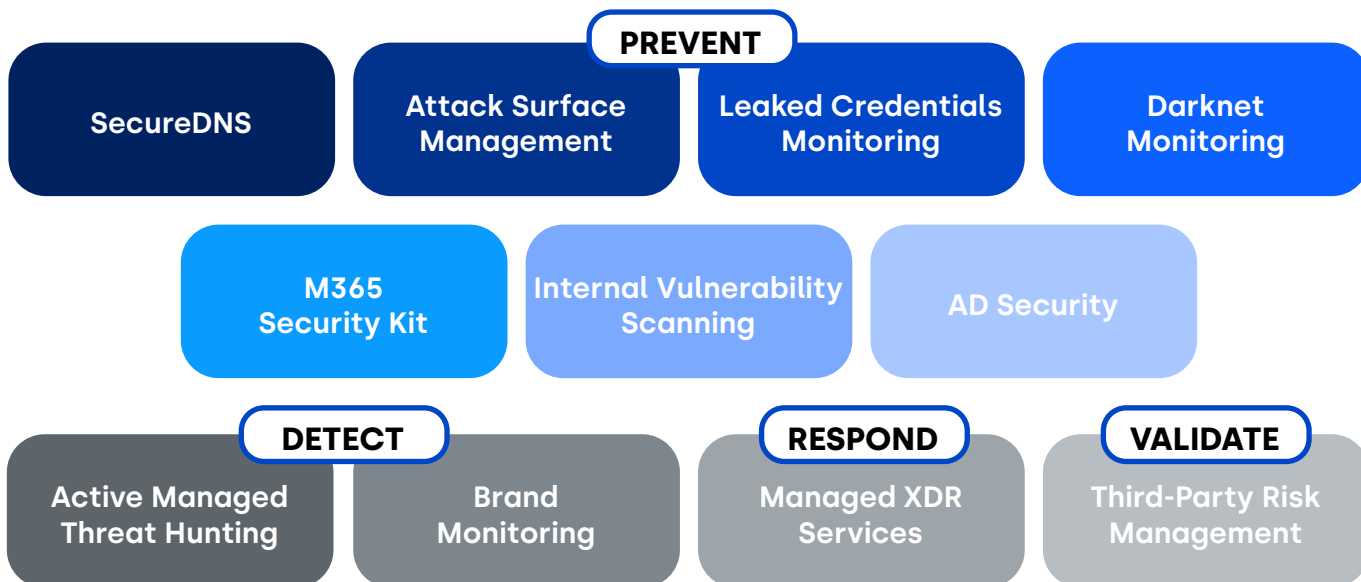
Konzentrieren Sie sich auf Ihre Kernaufgaben, während wir uns um die Überwachung kümmern.

¹ SpyCloud 2024 Annual Identity Exposure Report

Kontinuierliche Überwachung Ihres digitalen Perimeters

Der **Managed Service** von Secutec SecureSIGHT bietet die kosteneffizienteste Lösung, die die wichtigsten Aspekte des Lebenszyklus eines Cyberangriffs abdeckt, indem sie eine breite Palette von Angriffsvektoren und Indikatoren für eine Kompromittierung analysiert. Das **Secutec Security Operations Center (SOC)** sammelt alle Daten über mögliche Angriffe, fügt den Warnungen einen Kontext hinzu und liefert Ihnen verwertbare Daten und interpretierte Erkenntnisse.

Secutec SecureSIGHT nutzt Ihre bestehende Sicherheitsinfrastruktur und bietet **11 verschiedene Module**, die auf Ihre spezifischen Anforderungen zugeschnitten sind.



MySecutec | Übernehmen Sie die Kontrolle über Ihre Cybersicherheit

Das MySecutec-Portal ermöglicht es Ihnen, sich stärker mit den Sicherheitsergebnissen Ihrer Organisation auseinanderzusetzen. Es bietet ein **übersichtliches, intuitives Dashboard**, das **alle wichtigen Sicherheitsdaten an einem Ort** zusammenführt – darunter Assets, Berichte, Bedrohungen und akzeptierte Risiken.

Mit umsetzbaren Erkenntnissen können Sie kritische Schwachstellen schnell erkennen, priorisieren und beheben, das Risikoniveau Ihrer Assets verfolgen und Bedrohungen mithilfe integrierter Notizen, Filter- und Exportoptionen nachverfolgen. Echtzeitwarnungen für kritische Bedrohungen werden per E-Mail zugestellt, sodass Sie stets informiert sind und sofort handeln können.

Ihr zentrales Sicherheitszentrum, immer griffbereit

Secutec bringt bald die neue MySecutec-App auf den Markt, mit der Ihre Cybersicherheit **jederzeit und überall verfügbar** ist.

- Sofortiger Zugriff auf Ihre Cybersicherheitsdaten
- Echtzeit-Warnungen bei kritischen Schwachstellen
- Live-Daten zu Ihrem Sicherheits-Score, Bedrohungen und Risiken
- Überblick über und Verwaltung von Zugangsdaten-Lecks auf einen Blick

Kontaktieren Sie uns für weitere Informationen.

