

The ACP logo is located in the top left corner, consisting of the letters 'ACP' in a bold, italicized, sans-serif font. Below the text is a horizontal red bar. The background of the entire page is a photograph of a large, white, dome-shaped observatory structure on a dark, rocky hillside under a starry night sky.

ACP

ACP SOC-Observer

Bleiben Sie Angreifer*innen stets einen Schritt voraus. Mit unserem ACP SOC-Observer identifizieren Sie die externen Angriffspunkte Ihrer Infrastruktur. Umfangreiche Analysen und Empfehlungen von unseren Expert*innen unterstützen Sie auf Ihrem Weg zur Cyberresilienz.

**IT for
innovators.**

Cybersecurity à la carte



Erhalten Sie einen individuellen 360 Grad Blick auf Ihre Cyberrisiken! Nutzen Sie unseren ACP SOC-Observer ganz nach Ihren Bedürfnissen. Damit Sie von maximaler Flexibilität profitieren, haben wir unseren Service modular aufgebaut:



EXTERNAL

01

Cyber Threat Analysis



THREAT

02

External Attack Surface Management



SURFACE

03

Digital Risk Protection

01 Cyber Threat Analysis

Mit dem Cyber Threat Analysis Modul erweitern wir den Umfang der SOC Analyse und nehmen aktuelle Bedrohungen ins Visier. Sollten wir Sicherheitsrisiken entdecken, wird in gewohnter höchster Qualität ein Alarm ausgelöst. Unser Ziel ist es, die Bedrohung so früh wie möglich zu erkennen, die Vorgehensweise zu verstehen und einen möglichen Angriff zu unterbinden.

02 External Attack Surface Management

Wagen Sie den Blick von außen! Die externe Sicht auf Ihre IT-Infrastruktur, ihre Analyse und das Auffinden von Schwachstellen bilden die Basis für das Vorgehen potenzieller Angreifer*innen. Nutzen Sie diese Kenntnisse über Ihre Angriffsfläche für Ihre Verteidigung. Bei diesem Modul scannen und erkennen wir fortlaufend Ihre externe Angriffsfläche. Mit einem detaillierten Reporting und Empfehlungen zu Gegenmaßnahmen erhöhen Sie Ihre Sicherheit und verringern die Angriffsmöglichkeiten.

03 Digital Risk Protection

Entdecken Sie sensible Informationen Ihres Unternehmens! Ziel der Digital Risk Protection ist es, sensible Unternehmensdaten im Clear-, Deep- und Darkweb aufzufinden. Damit wir relevante Daten wie kompromittierte Credentials, Personal data (PII), Proprietary Code (Intellectual Property) oder Kreditkarteninformationen zuverlässig identifizieren, werden umfangreiche Datenquellen eingebunden und laufend gescannt. Entdecken wir sensible Informationen, bewerten unsere Expert*innen deren Relevanz und kontaktieren Sie umgehend mit passenden Maßnahmen.

Voraussetzungen

- Zustimmung zu einem initialen passiven Scan, um die relevante Assetanzahl für die Lizenzierung zu bestimmen
- Ausreichende Lizenzierung der Assets in Scope des Services
- Bereitstellung der relevanten Informationen wie Hauptdomäne und VIP User
- Cyber Threat Analysis Modul: Eines der SOC Services „SOC-ACTAS“ oder SOC-Sentinel“

Ihr Nutzen

- > **Frühzeitige Abwehr von Cyberangriffen:** Mit dem ACP SOC-Observer identifizieren Sie die Angriffspunkte Ihrer IT-Infrastruktur, um Angriffe frühzeitig zu erkennen und zu unterbinden sowie zukünftige Cyberangriffe zu verhindern.
- > **360-Grad-Blick auf Cyberrisiken:** Durch einen ganzheitlichen Blick auf Ihre Cyberrisiken können Sie gezielt Maßnahmen ergreifen.
- > **Modulare Flexibilität:** Der ACP SOC-Observer ist modular aufgebaut, sodass Sie den Service gemäß Ihren individuellen Bedürfnissen nutzen können.
- > **Externe Sicht auf Ihre Infrastruktur:** Durch die externe Sicht auf Ihre Infrastruktur identifizieren Sie Schwachstellen und reduzieren Angriffspunkte.
- > **Auffinden sensibler Unternehmensdaten:** Sensible Unternehmensdaten werden im Clear-, Deep- und Darkweb aufgespürt, um mögliche Gefahrenquellen zu identifizieren.



Sie möchten mehr zum ACP SOC-Observer erfahren?

Dann wenden Sie sich bitte an:
security@acp.at



acp.at/soc