aroundsec

SECURITY OPERATIONS CENTER

ANGRIFFE ERKENNEN

AROUND IT-Security GmbH | Tel: +49 7266 44 79 79 0 | Mail: info@aroundsec.de

IHR SCHUTZNIVEAU STEHT BEI UNS IM FOKUS

WER SIND WIR

Die AROUND IT-Security GmbH, auch bekannt als aroundsec, macht mittelständische Unternehmen und Kommunen deutlich widerstandsfähiger gegen Cyberkriminalität.

Die IT-Systeme werden sowohl aus der Sicht eines potenziellen Angreifers (Red Team) als auch aus Sicht eines IT-Administrators (Blue Team) analysiert. Denn die meisten Unternehmen und öffentlichen Einrichtungen sind nur unzureichend geschützt und somit ein besonders lohnendes Ziel für Angreifer.

Unser Fokus liegt besonders auf den häufigsten und schwer-wiegendsten Angriffsarten. Sollte ein Angriff erfolgreich sein, unterstützen wir unsere Kunden zudem dabei, ihre Systeme wiederherzustellen sowie wichtige Daten und Beweise zu sichern.

Unser erfahrenes Expertenteam setzt über gängige Sicherheits-standards hinausgehende Methoden ein, um effektiven Schutz gegen Cyberangriffe zu gewährleisten. Dabei nutzen wir neueste Techniken und Erfahrungen, um sowohl die Wahrscheinlichkeit als auch den potenziellen Schaden von Angriffsarten zu minimieren.

SOC

ANGRIFFE ERKENNEN

Bei der Erkennung von Angriffen sollte nichts dem Zufall überlassen werden: Mit unserem maßgeschneiderten SIEM (Security Information and Event Management) inkl. XDR bieten wir Ihnen eine umfassende Lösung für Sicherheitsmonitoring, Active Response und Schwachstellenmanagement.

Unser Ansatz ist dabei klar: Das Security Operations Center (SOC) ist Ihre erste Verteidigungslinie gegen Cyberbedrohungen. Mit modernsten OpenSource-Technologien und proaktiven Sicherheitsmaßnahmen schützen wir Ihre Organisation rund um die Uhr vor Angriffen.

Dabei sind wir in der Lage, ein besonders ressourcen- und kostenschonendes SOC einzuführen. Unser System ermöglicht es Ihnen, durch die gezielte Korrelation von Event-Logs, potenzielle Sicherheitsverstöße und Angriffe frühzeitig zu erkennen. Dadurch wird nicht nur die Sichtbarkeit von möglichen Angriffen erheblich verbessert, sondern es ermöglicht auch eine proaktive Reaktion auf Sicherheitsvorfälle.

Leistungsübersicht:

- **Erkennung**: Frühzeitiges Erkennen und Abwehren von Angriffen sowie das Identifizieren und Beheben von Schwachstellen.
- **OpenSource-SIEM:** Mit unserem SIEM inkl. XDR überwachen und analysieren wir sicherheitsrelevante Daten in Echtzeit.
- **Installation:** Wir richten das SOC vollständig in unserem deutschen Rechenzentrum für Sie ein und sorgen dafür, dass es optimal läuft.
- **Integration:** Verbinden Sie Ihre Endgeräte, Server und Netzwerkinfrastruktur nahtlos mit unserem SOC.
- **Compliance:** Unterstützung bei der Einhaltung relevanter Sicherheitsstandards und -vorschriften.
- **Proaktive Benachrichtigungen:** Wir melden uns proaktiv bei Ihnen, wenn Bedrohungen oder Sicherheitsverstöße identifiziert werden.
- **Statusberichte:** Sie erhalten regelmäßig detaillierte Berichte mit allen wichtigen und aktuellen Informationen zur Sicherheitslage.