[abtis]
DIGITALE ZUKUNFT

SOC AS A SERVICE

Das Rundum- Sicherheitspaket

In einer Welt, in der digitale Bedrohungen keine Grenzen kennen, ist ein proaktiver und ganzheitlicher Schutzansatz für Unternehmensnetzwerke unerlässlich. SOC as a Service bietet genau das: eine umfassende Sicherheitslösung, die rund um die Uhr für Sie im Einsatz ist. Mit abtis SOC as a Service erhalten Sie nicht nur eine kontinuierliche Überwachung Ihrer Systeme, sondern auch die Gewissheit, dass auf jede Bedrohung sofort reagiert wird – und das mit der Expertise und den fortschrittlichen Technologien eines dedizierten Security Operations Center.

Unser Service zeichnet sich durch Echtzeiterkennung und -reaktion auf Bedrohungen, kontinuierliche Überwachung und die Zusammenführung von Log-Daten sowie einen ganzheitlichen Überblick über Ihre Sicherheitslage aus.

Wir verstehen die Herausforderungen mittelständischer Unternehmen und haben unseren SOC as a Service speziell darauf ausgerichtet, um Ihnen eine umfassende, effektive und effiziente Sicherheitsüberwachung zu gewährleisten.

Mit abtis an Ihrer Seite können Sie sich darauf verlassen, dass Ihr Unternehmen gegen die komplexen Bedrohungen von heute gewappnet ist. Unser Expertenteam sorgt für eine lückenlose Überwachung Ihrer Nodes und Services, schützt Ihre Cloud-Umgebung und stellt sicher, dass Sie den Compliance-Standards stets gerecht werden. Wir bieten nicht nur Alarmierung und Reaktion auf Sicherheitsvorfälle, sondern auch proaktive Threat Hunting und Schwachstellen-Scans, um Ihr Unternehmen bestmöglich zu schützen.

Key Facts

- 100 % Sicherheit durch permanente Überwachung
- Identifizierung und schnelle Erkennung der Schwachstellen (Threat Hunting)
- 24/7 Reaktionsfähigkeit und Alarmierung bei kritischen Sicherheitsvorfällen

[abtis]
DIGITALE ZUKUNFT

Umfassender Schutz im digitalen Zeitalter

Ein leistungsfähiges Security Operations Center (SOC) ist entscheidend für die Cyber-Sicherheit eines Unternehmens. Es sollte über das eigene Netzwerk hinaus alle digitalen Zugangspunkte wie mobile Geräte, Cloud-Services und IoT-Technologien überwachen.
Die Effektivität des SOCs basiert auf einer breiten Datenerfassung, die eine schnelle Reaktion auf Bedrohungen ermöglicht. Zudem sind tiefgehende Analysen notwendig, um komplexe Cyberangriffe zu enttarnen. Automatisierung spielt eine wesentliche Rolle, um die Flut an Sicherheitswarnungen zu bewältigen und Experten die Konzentration auf strategische Abwehrmaßnahmen zu erlauben. Ein modernes SOC zeichnet sich durch Anpassungsfähigkeit an die sich ständig verändernde Bedrohungslandschaft aus und bietet mehr als nur traditionelle Netzwerküberwachung – es ist ein umfassender Wächter über alle digitalen Pforten eines Unternehmens.

Auszug aus unseren Leistungen

Überwachung (Monitoring)

- Monitoring des Compliance & Konfigurationsstatus der eingebundenen Nodes und Services rund um die Uhr
- Überwachung & Alarmierung bei kritischen Anmeldevorgängen von Useraccounts (sofern Defender for Identity implementiert)
- Überwachung des Server-Schutzstatus der eingebundenen Windows- und Linuxnodes
- Überwachung von Admin- und Ressourcenverhalten, sowie Berechtigungsänderungen in Cloudinfrastrukturen
- Überwachung und proaktive Bearbeitung von Azure Security Alerts
- Monitoring der Umgebung hinsichtlich Risiken basierend auf Compliance-Standards (ISO)
- Monitoring der eingebundenen IT-Landschaft inklusive Attack Path Analysis
- Überwachung von CRM / ERP Systemen auf Anomalien und Security Alerts sofern angebunden und supported
- Regelmäßige Analyse der Sicherheitslage Ihrer Azure IaaS mit Handlungsempfehlungen.
- Analyse von Netzwerktraffic auf Anomalien von angebundenen Firewall Systemen
- Überwachung und Benachrichtigung bei Anomalien von kundenspezifischen Systemen über Syslog Streaming

[abtis]
DIGITALE ZUKUNFT

Erkennung (Detection)

- Identifizierung verdächtiger Benutzer- und Serveraktivitäten, sowie verdächtiges Anmeldeverhalten bei angebundenem Microsoft Azure AD
- Alarmierung bei unautorisierten Device im Unternehmensnetzwerk bei angebundener NAC-Lösung
- Proaktives Threat Hunting bei Zero Day Schwachstellen hinsichtlich „Indicators of Compromise“ (IOCs)
- Monatlicher Schwachstellen Scan auf eingebunden Windows-, MacOS- und Linuxnodes
- Alarmierung bei high & critical Schwachstellen auf eingebundenen Systemen mit Handlungsempfehlung
- Automatisiertes Hunting von neuen Sicherheitsrisiken

Reaktion (Response)

- Alarmierung bei Security Incidents mit entsprechenden Handlungsempfehlungen durch SOC-Analysten 24/7/365
- Proaktive Reaktion bei kompromittierten Useraccounts 24/7/365 (Sperren, Password Reset, MFA Enforcement)
- Proaktive Meldung kritischer Sicherheitsvorfälle im Zusammenhang mit eingebundenen Services
- Definition und Bereitstellung von Action-Plänen im Falle von Security Incidents auf eingebundenen Services

Vorbereitung / Administration

- Initiale Einbindung von Services und Nodes in das abtis CDOC
- Backend-Vorbereitung für Onboarding der Services und zusätzlicher Nodes via Defender for Cloud
- Verwaltung und Pflege der Microsoft Defender for Endpoints Server-Konfiguration
- Integration von Connectoren (Cisco Meraki, Palo Alto, SAP u.a.) gemäß Kundenwunsch
- Anbindung von Firewall-Systemen bezüglich IPS, IDS, Gateway-Antivirus

Unterstützende Leistungen

- Monatliche Konfigurationsempfehlung für in Defender for Cloud integrierte Nodes
- Dashboard-Bereitstellung zum Serverpatchlevel der Systeme

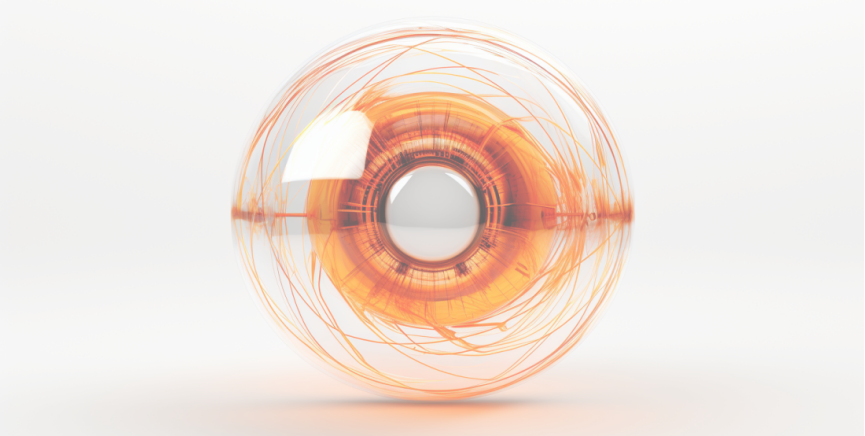
Ihr starker IT-Partner im Mittelstand

abtis verfügt über mehr als 20 Jahre Erfahrung in der Planung und dem Betrieb von Microsoft Infrastrukturen und betreut mehr als 200.000 Anwender der Cloudplattformen Microsoft 365 und Azure.

Ausgezeichnet als Microsoft Solutions Partner und mit 13 Advanced Specializations sind wir einer von zehn Fokuspartnern von Microsoft für den Mittelstand in Deutschland. Damit setzen wir ein starkes Zeichen als verlässlicher Partner und Vorreiter in der IT-Branche.

Die Expertise von abtis wird weiter unterstrichen durch die Mitgliedschaft in der **Microsoft Intelligent Security Association** und die Zertifizierung als **Microsoft Certified Professional für Security**. Mit den Advanced Specializations in „Threat Protection", „Identity and Access Management" sowie „Information Protection and Governance" hebt sich abtis deutlich von der Konkurrenz ab.

Als einer von nur vier deutschen Microsoft Partnern ist abtis zudem als Verified **MXDR Solution Partner** anerkannt. Der Managed Security Service von abtis, eine von Microsoft verifizierte MXDR-Lösung, bietet eine umfassende Serviceabdeckung, die den gesamten Microsoft Security Stack einschließt. Dieses Angebot unterstreicht das Engagement von abtis, durchdachte Managed Security Services speziell für den Mittelstand zu realisieren.



Kontakt
+49 7231 4431 - 100
vertrieb@abtis.de