

Axians MDR für Endpoints

Mit unserem Service reduzieren Sie proaktiv die Angriffsflächen Ihres Unternehmens, verhindern Malware-Infektionen, erkennen und entschärfen potenzielle Bedrohungen in Echtzeit und automatisieren Reaktions- und Abwehrmassnahmen.



SCHUTZ VOR DEM UNBEKANNTEN

Ihr erster Schritt zu einer ganzheitlichen Cyber-Security-Betrachtung

Axians Active MDR (Managed Detection and Response) ist ein Cyber Security Service, der führende Technologie für Endpoints und menschliches Fachwissen kombiniert, um Bedrohungen zu finden, zu überwachen und darauf zeitgerecht zu reagieren.

Unser Service hat ein ganz klares Ziel vor Augen: **die Bewältigung der steigenden Herausforderungen im Bereich Endpoint Security**. Axians Active MDR bildet dabei den Einstieg zu einem vollwertigen Managed SOC (Security Operations Center) Service.

Was beinhaltet Axians MDR für Endpoints?

Axians MDR für Endpoints ist ein Zusammenspiel aus der Technologie unseres Partners SentinelOne und unseren Managed Service Leistungen, welche durch unser Cyber Security Team aus unserem modernen IT/OT SOC im up-townBasel erbracht werden.

Operative Exzellenz durch Kombination von Technologie und Service

Die Bereitstellung der Technologie erfolgt zum Einen über die Single-Agent-, Single-Codebase- und Single-Konsolen-Architektur, wobei der Hauptzweck darin besteht, bekannte und unbekannte Bedrohungen proaktiv zu identifizieren – beispielsweise bisher unbekannte Infektionen, die sich direkt über Endpoints in das Unternehmen einschleichen. Zum Anderen stützt sich die erweiterte Analytik auf verteilte künstliche Intelligenz, welche Muster und Anomalien erkennt. Dies funktioniert sowohl On-Premise als auch in der Cloud und auf allen relevanten Betriebssystemen. Bei verdächtigem Verhalten sendet SentinelOne automatisch Warnungen an das Axians Cyber Security Team, so dass diese untersucht und weitere Massnahmen ergriffen werden können.



Unser Managed Service beinhaltet folgende Leistungen:

- ▶ **Design und Implementierung** der SentinelOne Endpoint Security-Lösung in Cloud- und/oder On-Premise-Rechenzentren
- ▶ **Onboarding** in das Axians Security Operations Center
- ▶ Erstellung der **operativen Playbooks und Regeln**
- ▶ Proaktive **Überwachung und Reaktion** auf Cyber Bedrohungen 24x7x365
- ▶ **Empfohlene Vorgehensweise** für jedes Ereignis, klassifiziert nach Risikoprofil
- ▶ **Geführte Anweisungen** zur Fehlerbehebung mit Fernkorrektur und Rollback
- ▶ **Regelmässige Überprüfung** der Cyber-Security-Umgebung
- ▶ **Installation, Konfiguration, Upgrades, Tests und Wartung** von Endpoint-Konsolen
- ▶ Regelmässiges und bedarfsgesteuertes Scannen zur **kontinuierlichen Suche nach Sicherheitsproblemen**
- ▶ **Beratung** zum Schutz vor Datenverlusten und Disaster-Recovery-Strategien
- ▶ **Kundenspezifische Lösungen und Skripte** zur Steigerung der Effizienz und Verringerung der Notwendigkeit menschlicher Eingriffe (Automatisierung)
- ▶ **Implementierung und Anpassung von Reports** zur Schaffung von Transparenz für Ihre Cyber-Security-Organisation
- ▶ **Schulung und Wissensaustausch**

Axians MDR für Endpoints



Ihre Vorteile auf einem Blick

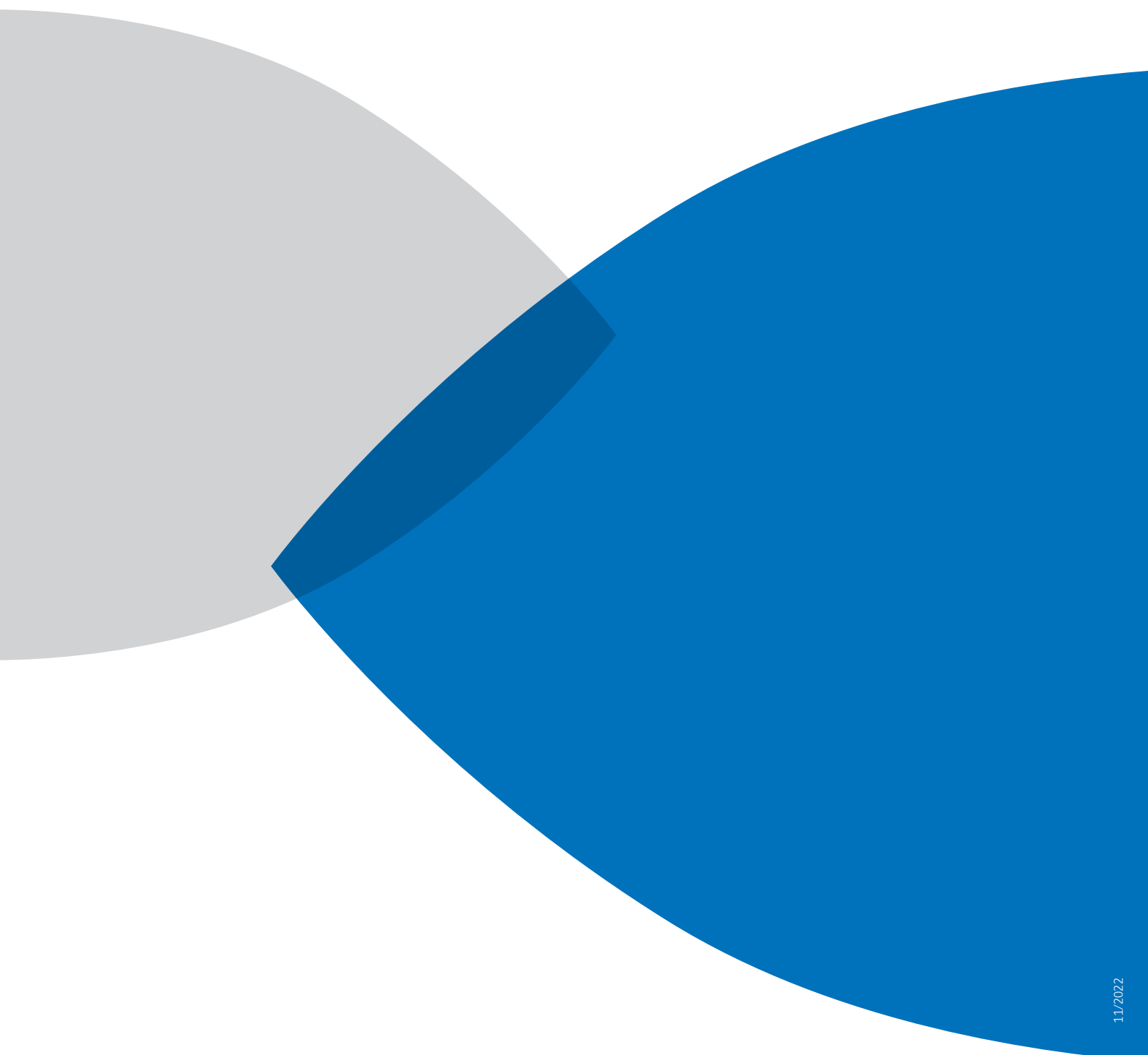
- ▶ **Schutz Ihres Unternehmens** gegen fortschrittliche Cyber Bedrohungen der Endpoints
- ▶ Sicherstellung der **Produktivität Ihrer Mitarbeiter** und **Wahrung des operativen Geschäftes**
- ▶ Zeitgerechte Identifikation von Angriffen und **Begrenzung der Auswirkungen**
- ▶ **Entlastung** Ihrer IT-Abteilung
- ▶ **Erhöhung der Security-Maturität** Ihres Unternehmens
- ▶ **Einsparungen** von OPEX durch Konsolidierung von Endpoint-Agenten
- ▶ Verringertes Risiko durch Angriffe und **reduzierte Zeit zur Behebung von Vorfällen**
- ▶ **Reduzierter Ausbau** von eigenen Cyber-Security-Mitarbeitern



IHR ANSPRECHPARTNER

Mathias Bücherl (CTO)

E-Mail: mathias.buecherl@axians.com



axians

Axians IT Services AG · Arlesheim · Rotkreuz · Zürich

Tel.: +41 61 716 70 70

E-Mail: info-ch.security@axians.com · www.axians.ch