axians

Axians MDR for Endpoints

The Axians Active MDR Service reduces attack surface, prevents malware infections, detects and mitigates potential threats in real-time and automates response and defense measurements.

One more step towards a holistic Cyber Security Strategy

Axians Active MDR (Managed Detection and Response) is a cyber security service that combines leading endpoint technology and human expertise to detect, monitor and respond to threats in a timely manner.
With the growing challenges in the area of endpoint security **Axians MDR for Endpoints is the entry point to a fully-fledged managed SOC (Security Operations Center) service.**

What does Axians MDR for Endpoints?

Axians Active MDR is a combination of technology (SentinelOne) and the Axians managed SOC services.
Our cyber security team in the IT/OT SOC in uptownBasel provides experienced security analysis and cutting-edge expertise.

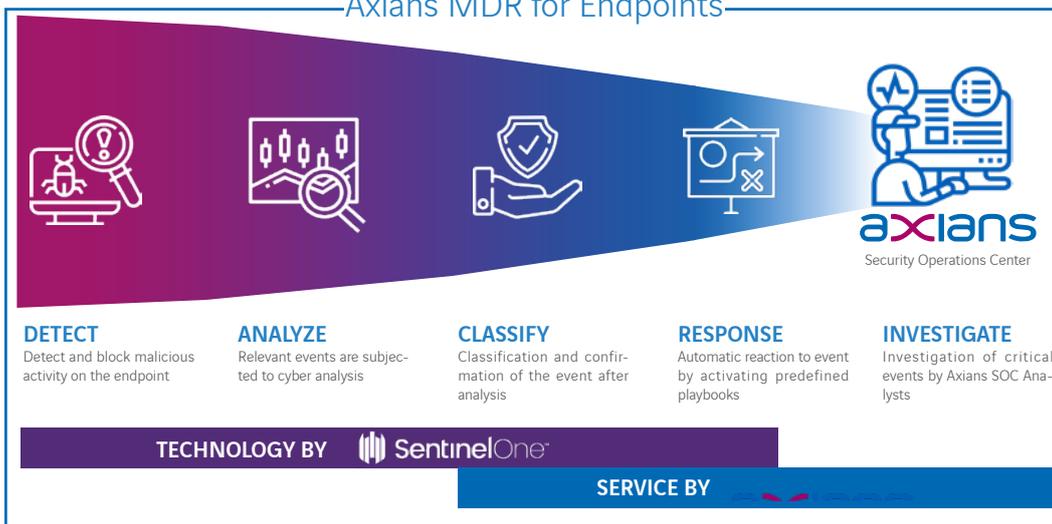## Operational excellence through combination of technology and service

The technology is deployed using single-agent, single-codebase and single-console architecture with the main purpose to proactively identify known and unknown threats attacking your company sneaking directly into your network via endpoints. Through advanced analytics, using detection methods that rely on distributed artificial intelligence, it is possible to detect malware and suspicious behaviour based on patterns and anomaly monitoring. In case of an incidence SentinelOne automatically sends alerts to the Axians Cyber Security team where further investigation will take place to reduce the possibility of false-positives. Further action plans will be executed based on pre-defined playbooks and customer-specific case scenarios.

Our Managed Service at a Glance:

▸ **Design and implementation** of the SentinelOne Endpoint Security solution in cloud and/or on-premise data centres

▸ **Onboarding** into the Axians Security Operations Center

▸ Definition of **operational playbooks and rules**

▸ Proactive **monitoring and response** to cyber threats 24x7x365

▸ **Recommended course of action** for each event, classified by risk profile

▸ **Guided troubleshooting** instructions with remote correction and rollback

▸ **Regular review** of the cyber security environment

▸ **Installation, configuration, upgrades, testing and maintenance** of endpoint consoles

▸ **Regular and on-demand scanning** to continuously look for security issues

▸ **Advice** on data loss prevention and disaster recovery strategies

▸ **Customised solutions** to increase efficiency and reduce the need for human intervention (automation)

▸ **Implementation and customisation of reports** to create transparency for your cyber security strategy

▸ **Training and knowledge sharing**

Axians MDR for Endpoints

DETECT
Detect and block malicious activity on the endpoint

ANALYZE
Relevant events are subjected to cyber analysis

CLASSIFY
Classification and confirmation of the event after analysis

RESPONSE
Automatic reaction to event by activating predefined playbooks

INVESTIGATE
Investigation of critical events by Axians SOC Analysts

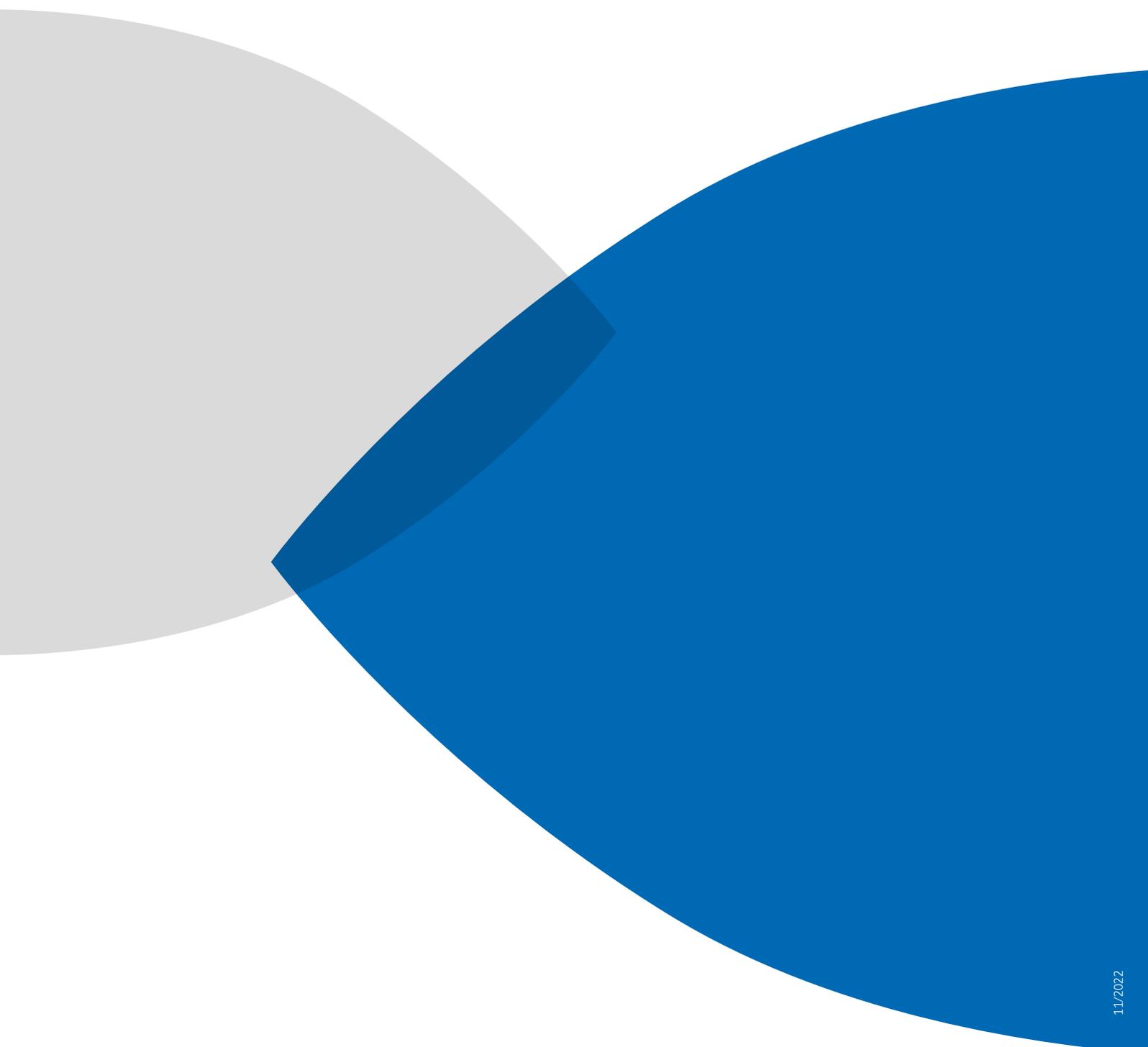TECHNOLOGY BY **SentinelOne**

SERVICE BY

Your Benefits at a Glance

▸ **Protection for your business against** advanced cyber threats to endpoints

▸ **Productivity of your employees** and **preserving your business operations**

▸ Identification of attacks in a timely manner to **eliminate or limit business impact**

▸ **Reduction of workload** of your IT departments

▸ Increase of your **company`s security maturity**

▸ **Less OPEX** by consolidating endpoint agents

▸ **Reduction** of in-house headcounts cyber security teams

YOUR CONTACT PERSON

Mathias Bücherl (CTO)

E-Mail: mathias.buecherl@axians.com