the Impact Team

Axonius Cybersecurity Asset Management Platform

Overview:

Axonius supplies a Cybersecurity Asset Management Platform with which businesses can get full visibility and control of their IT assets. A new platform that's truly game-changing, consolidating with existing security and management tools through correlating together all asset data in order to create a single source of truth across all connected devices, users, and cloud instances.

Axonius therefore enables organisations to automate the taking of an inventory of their assets, analysis of risks, and enforcement of security policies—all this helps in streamlining security operations and thus reducing the attack surfaces for organisations.

Service Objective:

Our assessment helps organisations identify potential vulnerabilities within their systems and networks. Allowing them to proactively address and mitigate risks before they are exploited by malicious actors. Armed with this knowledge, organisations can make informed decisions regarding cybersecurity investments, prioritise risk mitigation efforts, and allocate resources effectively.

Our cyber risk assessment service is an essential step towards building a resilient and secure digital infrastructure, safeguarding valuable assets, and ensuring the long-term success and growth of an organisation in today's high-risk cyber landscape

Key Features:

A comprehensive report and presentation is produced which details various aspects of the organisation's cybersecurity posture, including areas such as:

- IT Asset management
- Access rights usage
- Vulnerability & patch management
- Licence usage
- Accuracy of CMDB

The Impact Team Process:

Deploy On-premises Data Collectors

- Installation: Set up Axonius Data Collectors on internal servers to bridge data between on-premises assets and Axonius.
- Configuration: Specify network settings and credentials for the Data Collectors to ensure comprehensive asset communication.

Scan In-scope Assets

- Define Scope: List all assets to be managed, including devices, applications, and network components.
- Automated Discovery: Activate Axonius' scanning to catalog assets and enable continuous asset monitoring.

Connect via Read-only API to In-scope Applications

- API Integration: Set up read-only API connections with applications to safely import asset data into Axonius.
- Authentication and Authorization: Implement secure authentication for API access, ensuring data integrity.

Assess External Facing Assets

- External Asset Identification: Pinpoint internet-accessible assets for heightened security scrutiny.
- Vulnerability Scanning: Assess these assets with vulnerability scanners or Axonius' features to identify risks.

Run Through a Comprehensive Security Questionnaire

- Stakeholder Engagement: Distribute the questionnaire to gather cross-departmental security insights.
- Analysis and Action Plan: Analyze responses to develop an action plan for enhancing security practices using Axonius.

Commercial Offering:

£15,000 for 6-week duration

- Ignition provide engineering support