CHILLISOFT
Cybersecurity specialists

ARMIS®

Chillisoft Services Health Check Document for Customers Using Armis Cybersecurity Services

Overview

This health check document is designed for customers utilizing Armis cybersecurity services, specifically the Armis Centrix™ platform, as of August 22, 2025. It assesses the implementation, performance, and effectiveness of Armis services in protecting the customer's digital and physical assets, with a focus on asset visibility, vulnerability management, and threat mitigation. The evaluation draws on information from the Armis website (https://www.armis.com/), related web resources, and best practices for cybersecurity service health checks.

Chillisoft (www.chillisoft.net) a specialist technical value-added distributor for Armis in ANZ has been contracted to provide health check services for all existing and new customers of Armis in the region utilizing our local Armis certified engineers. This additional local capability is designed to provide more support for partners and customers of Armis.

Why Your Business Needs an Armis Health Check

In today's hyper-connected world, your enterprise is surrounded by a growing ecosystem of IT, OT, IoT, and cloud-connected devices. Armis provides unmatched visibility and security across this landscape—but even the most powerful platforms need regular optimization to deliver peak performance.

An Armis Health Check is not just maintenance—it's a strategic advantage.

Maximize Visibility

Ensure your organization is seeing *everything*—from unmanaged devices to shadow assets. A health check validates that your asset inventory is complete, accurate, and dynamically updated, so you're never flying blind.

Optimize Performance

Fine-tune configurations, integrations, and automation workflows to ensure Armis is working as efficiently as possible. This means faster threat detection, smoother incident response, and better alignment with your business processes.

Strengthen Security Posture

Identify gaps in threat detection, vulnerability prioritization, and policy enforcement. A health check helps you proactively address risks before they become incidents—protecting your reputation and bottom line.

Improve Reporting & Compliance

Ensure dashboards, alerts, and compliance reports are tailored to your business needs. Whether it's NIST, CIS, GDPR, or internal standards, a health check ensures your reporting is accurate, actionable, and audit ready.

Enhance Integrations & Automation

Validate that Armis is seamlessly integrated with your SIEM, CMDB, ITSM, and other tools. A health check ensures data flows are secure, automated, and delivering value across your security ecosystem.

Ensure Proper Access & Governance

Review user roles, permissions, and access controls to prevent privilege creep and ensure accountability. This is critical for maintaining operational integrity and meeting regulatory requirements.

The Bottom Line

An Armis Health Check empowers your business to:

- Reduce risk
- Improve operational efficiency
- Strengthen compliance
- Maximize ROI from your Armis investment

Security isn't static—neither should your platform be. Let's make sure Armis is working as hard as you are.

What is included in your Armis Health Check?

Platform & Subscription Review

- Confirm active modules (Asset Management, Threat Detection, Vulnerability Prioritization, Secure Remote Access, Compliance Reporting)
- Review license usage vs. entitlements
- Check subscription expiration and renewal dates

Asset Management

- Validate full asset inventory across IT, OT, IoT, IoMT, and cloud environments
- Ensure CMDB enrichment is functioning correctly
- Identify stale, duplicate, or unmanaged assets
- Confirm dynamic asset classification and tagging rules
- Review asset scoping per business unit or site

Threat Detection & Response

- Verify anomaly detection and behavioural baselining are active
- Review Indicators of Compromise (IOC) coverage
- Validate threat forensic data collection and incident response workflows
- Check alerting and notification configurations

Vulnerability Prioritization (VIPR Pro)

- Confirm contextual vulnerability prioritization is enabled
- Review deduplication and risk scoring accuracy
- Validate remediation workflows and ticketing integrations
- Ensure alignment with critical asset protection strategies

Secure Remote Access (SRA)

- Audit identity-driven access policies
- Review session recording and audit trail configurations
- Validate least-privilege enforcement across OT/IoT environments
- Confirm firewall and protocol access rules are optimized

Policy Enforcement & Compliance

- Review automated policy actions (e.g., scan triggers, ticket creation)
- Validate mapping to compliance frameworks (NIST, CIS, GDPR, MITRE, etc.)
- Check internal and external compliance reporting dashboards
- Ensure policy wizard configurations reflect current security posture

Integrations & Automation

- Confirm integrations with SIEM, CMDB, EDR, ITSM, SOAR, and cloud platforms
- Review API usage and access controls
- Validate automation workflows (e.g., asset onboarding, alert enrichment)
- Ensure synchronization with third-party vulnerability and asset tools

User Access & Roles

- Audit user accounts and role assignments
- Remove inactive or unnecessary accounts
- Validate RBAC configurations and site-level access controls
- Review access approval workflows and SAML settings (if applicable)

General Maintenance

- Check for Armis platform updates or announcements
- Review system logs for errors or warnings
- Document changes and findings from the health check
- Confirm operational resilience strategies are in place