BOHIOSYSTEM

SERVICE DATASHEET · BOHIOSYSTEM

Cybersecurity

We protect operations with controls proportionate to real risk: assessment, hardening, monitoring, and incident response.

DOCUMENT
BS-SVC-12

VERSION
1.0

DATE
August 1, 2026

PREPARED BY
BohioSystem

THE SERVICE

> **Security isn't purchased, it's operated. An expensive firewall on an unsegmented network with shared passwords protects nothing.**

We assess an organization's real security posture, prioritize by risk, and execute the measures that reduce exposure: access control, system hardening, segmentation, monitoring, and response capability.

We always work under written authorization and a defined scope. Every technical test is carried out within the agreed limits and with a full report of the findings.

By risk
PRIORITIZATION, NOT A CHECKLIST

Authorized
WRITTEN SCOPE

Continuous
NOT A YEARLY SNAPSHOT

Actionable
WITH A REMEDIATION PLAN

01 What we solve

What we find most often in an initial assessment.

COMMON SITUATION	WHAT IT MEANS FOR THE BUSINESS
Shared credentials	Several people use the same administrative account, so no action can be attributed to anyone, and offboarding staff revokes nothing.
No second factor	Access to email, systems, and the cloud depends on a single password that is probably reused on other services.
Unpatched systems	Servers and devices with known vulnerabilities and a patch that has been available for months.
Backups reachable by an attack	The copies sit on the same network with the same credentials, so a mass encryption event takes them out too.
No visibility	There are no centralized logs, so if there was unauthorized access, no one would know or be able to reconstruct what happened.
No response plan	No one knows who to call, what to disconnect, or what to communicate if a ransom note shows up tomorrow.

02 What the service includes

01 Security assessment

An honest snapshot of the current state, with findings prioritized by real risk rather than theoretical severity.

Architecture review · Vulnerability analysis · Access and permissions review · External exposure · Executive and technical report

02 Identity and access management

The control with the best ratio between effort and risk reduction. It's almost always where we start.

Named individual accounts · Mandatory second factor · Least-privilege access · Corporate password manager · Periodic access reviews · Onboarding and offboarding procedure

03 System hardening

Reducing the attack surface of servers, devices, and exposed services.

Secure configuration per platform · Patch management · Disabling unnecessary services · Encryption in transit and at rest · Network segmentation

04 Monitoring and detection

Making sure there is a record of what happens, and someone watching it when something falls outside the norm.

Centralized logging · Event correlation · Endpoint detection · Prioritized alerts · Retention for investigation

05 Incident response

A procedure agreed on before the incident, because during the incident there is no time to write it.

Written response plan · Roles and contact tree · Containment and eradication · Verified recovery · Post-incident report and lessons learned

06 Culture and awareness

Most incidents start with someone clicking a link. It's the cheapest control and the most ignored.

Training by role · Phishing simulations · Understandable policies · No-blame reporting channel · Improvement measurement

03 How we work

In short stages, with something verifiable at the end of each one.

PHASE	WHAT HAPPENS	WHAT YOU KEEP
01 · Discovery	We understand the business, the current state and the real constraint.	Diagnosis and agreed scope.
02 · Design	We define the solution, its risks and its execution plan.	Architecture and milestone plan.
03 · Build	We implement in verifiable increments, not in a single delivery.	Functional progress per milestone.
04 · Go-live	Controlled deployment, testing and knowledge transfer.	Solution in production and team trained.
05 · Evolution	Operation, measurement and continuous improvement under a service agreement.	Periodic report and living roadmap.

04 What you receive

Assessment

- Executive report for leadership.
- Technical report with reproducible detail.
- Findings prioritized by risk.
- Remediation plan with estimated effort.

Implementation

- Controls applied and verified.
- Documented configuration.
- Updated access matrix.
- Before-and-after evidence.

Operation

- Monitoring with active alerts.
- Incident response plan.
- Containment procedures.
- Review schedule.

Policies

- Security policy tailored to the organization.
- Acceptable use standards.
- Onboarding and offboarding procedure.
- Training materials.

05 Technologies we work with

We choose the tool for the problem, not by trend or by agreement with a vendor.

WAZUH · CIS BENCHMARKS · OWASP · NMAP · OPENVAS · BURP SUITE · BITWARDEN · KEYCLOAK · WIREGUARD · PFSENSE · FAIL2BAN · LET'S ENCRYPT · VAULT · NIST CSF · ISO 27001

06 Engagement models

MODEL	HOW IT WORKS	WHEN IT FITS
Fixed project	Defined scope and deliverables, agreed price and timeline.	Bounded needs with a clear objective.
Monthly retainer	Reserved team capacity month to month.	Continuous evolution and sustained support.
Dedicated team	Profiles assigned exclusively under your direction.	Long programs or high workload.
Hour bank	Consumable hours with agreed priority.	Variable demand or one-off work.

07 Our commitments

COMMITMENT	HOW IT IS MET
Written authorization, always	No technical test is executed without scope, a time window, and authorization signed by someone with the authority to grant it.
We prioritize by real risk	A critical finding on a system with no data or exposure ranks behind a medium one on the system that handles billing.
No commercial fearmongering	We don’t inflate severities to sell more. The report distinguishes what’s urgent from what’s merely convenient.
Confidentiality	Findings are handled under a confidentiality agreement and delivered only to the agreed recipients.
Capability transfer	We explain every finding so the internal team can prevent it from happening again.

WHERE TO START ON A LIMITED BUDGET

Second factor on every access, named individual accounts with no sharing, isolated and tested backups, and up-to-date patches. Those four measures cost little and cover most of the incidents we see. Everything else comes after.

08 Next step

GET STARTED

A one-hour session, at no cost, to review your current situation and define together the minimum scope to start with.

CONTACT
contacto@bohiosystem.dev

WEB
bohiosystem.dev

DOCUMENT
BS-SVC-12 · v1.0