BASE4 SECURITY

*We help building a*

*more secure digital ecosystem!*

# Blue Team

## DATA SHEET

# Safety Diagnosis

Acquire an accurate cybersecurity diagnosis of your company in order to measure and prioritize risks in a short, medium and long term plan.

Through a work team that integrates different profiles (Audit, Networking, Ethical Hacking, Cloud Architects, among others), an Integral Security Diagnosis is performed in order to provide visibility and prioritization of the attack vectors and risks of the company. These are aligned with the business in order to draw up a Short and Medium Term Action Plan, prioritizing the risks, investment and remediation times for each vector.

- Security diagnosis is based on international frameworks such as CIS and NIST.
- The diagnosis is oriented to obtain the risks of the company's main attack vectors, such as perimeter equipment (FW, WAF, VPN), internal IPs, people, processes and architecture.
- The Diagnostic deliverables seek to obtain a current picture of the company's state of maturity in cybersecurity issues and to provide a roadmap for future projects and investments to be prioritized in this area.

# Vulnerability scanning

Get a snapshot of the main vulnerabilities of the customer's internal and external infrastructure in a short, cost-effective exercise.

Using third-party tools, BASE4 Security performs a Vulnerability Scanning exercise, attempting to obtain vulnerabilities from internal networks and public services.

The vulnerabilities discovered are delivered in these services in order of priority, as well as a recommendation for remediation. BASE4 Security can deliver a Remediation Plan in addition to these one shot services and also provide an online cloud platform for customers to manage vulnerabilities.

We market the One Shot service, Continuous service from our CyberSOC and the management of the customer's scanning platforms.

# Technology Assessment

Perform a configuration assessment of cybersecurity technologies such as Firewalls, WAF's, Ddos, EDR's, SIEM's, DLP's, among many others, in order to find improvements in them as well as to amortize such investment.

The main objective is to survey the different components of the Security technological architecture within the Network to determine in each component, the degree of separation of the Production, Development and Test environments, as well as their respective configurations and best practices.

Once the initial assessment is completed and the current situation is documented, the GAP between the current situation and the best practices based on industry and technology recommendations is determined.

Unused licenses and capabilities of the platform will also be detected in works so that they can be exploited by the client in the future and can better amortize its investment.

A hardening document of the platform is provided to the client and BASE4 Security can perform the fine tuning of the platform if the client requires it.

# Hardening

Execute the hardening of cybersecurity technology platforms through a fine tuning of the same, in search of a deeper protection of your organization.

The hardening of technologies helps to amortize their investment and protect the company against attackers. The service reduces human error and the organization's risks when dealing with platforms that are often strategic for the organization, such as Perimeter Firewalls, Antimalware or Information Leakage platforms.

The experience in implementation and support of these technologies, as well as the technical capacity of the BASE4 Security team, ensures a correct hardening of the same and the successful exploitation of the contracted licensing.

BASE4 Security has experience in more than 40 brands in the market, as well as in all cybersecurity technology platforms.

BASE4
SECURITY

www.base4sec.com