BOTECH

ISOPH VULNERABILITY

ISOPH VULNERABILITY: proactive vulnerability management

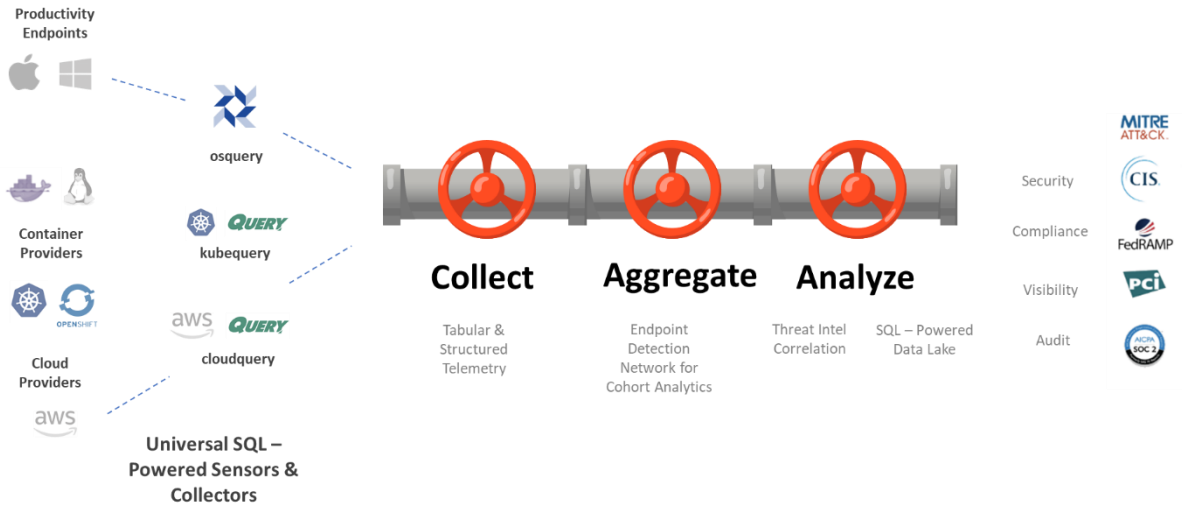
Today's challenge

In recent months, the time spent on websites, social networks, messaging programs, etc. has soared even more. But this increase has also created a new opportunity for cybercrime, which takes advantage of both, the increased exposure time to security risks and a user who is less alert, to carry out attacks at all possible points.

If we look at the workplace, the issue becomes even more complicated. With the increase in teleworking, many users are using their personal devices for corporate issues with all that this entails: less security, downloading of programs that are not 100% reliable.

ISOPH Platform

ISOPH was created for this reason, it is a technological platform that offers different services for managing the security status of equipment, thus making it possible to take measures to prevent



BOTECH

ISOPH VULNERABILITY

Benefits

-**It provides** a diagnosis of the vulnerabilities that your equipment currently suffers from.

• **Prevents** losses due to security incidents.

• **Easy and flexible** technology because it adapts to your infrastructure.

Features

• **Ease of use:** it requires only a few clicks to perform the scan.

• **Advanced** vulnerability detection.

• **Complete** vulnerability **scanning** with accurate, high-speed scanning.

What is ISOPH VULNERABILITY?

It is a service based on ISOPH technology that helps you keep your systems up to date and patched. It consists of continuous monitoring of vulnerabilities and periodic receipt of reports indicating whether there are any exploitable flaws in the protected systems.

ISOPH VULNERABILITY performs a security function against vulnerabilities that may arise to extend protection to devices, remote users and distributed locations anywhere.

Use ISOPH VULNERABILITY to:

- Automate vulnerability analysis and its continuous monitoring.
- Detect, assess, and prioritize vulnerabilities.
- Administrate network connection point security configurations.
- Strengthen Internet-oriented web servers.
- Remove unauthorized software.

ISOPH VULNERABILITY Compatibility

1. Collection of information

An event is generated from your device with the information and subsequently saved.

2. Filtration and analysis

Using the search commands the previously generated events are filtered and analyzed.

3. Sending of registered threats

Detected threats are sent along with a set of recommendations.

ISOPH only needs to check for changes when they occur on the device, e.g. when a program is downloaded. Therefore, it does not impair system performance as it does not require continuous execution.

ISOPH VULNERABILITY Compatibility

Operating systems supported: Windows		
Versions	**Language**	**Architecture**
Windows 10 Pro	Spanish/English/Portuguese	64-bit
Windows 8/ 8.1 Pro	Spanish/English/Portuguese	64-bit
Windows 7 Professional	Spanish/English/Portuguese	64-bit

Windows 32 bits and Vista not supported

Operating systems supported: Linux		
CentOS	7	64-bit
Ubuntu	18.04	
Ubuntu	20.04	

Operating systems supported: MAC

Compatibility with macOS is on our development roadmap.

Thank you!

www.botechfpi.com

Contact us:

info@botechfpi.com

T: + 34 911 74 35 66