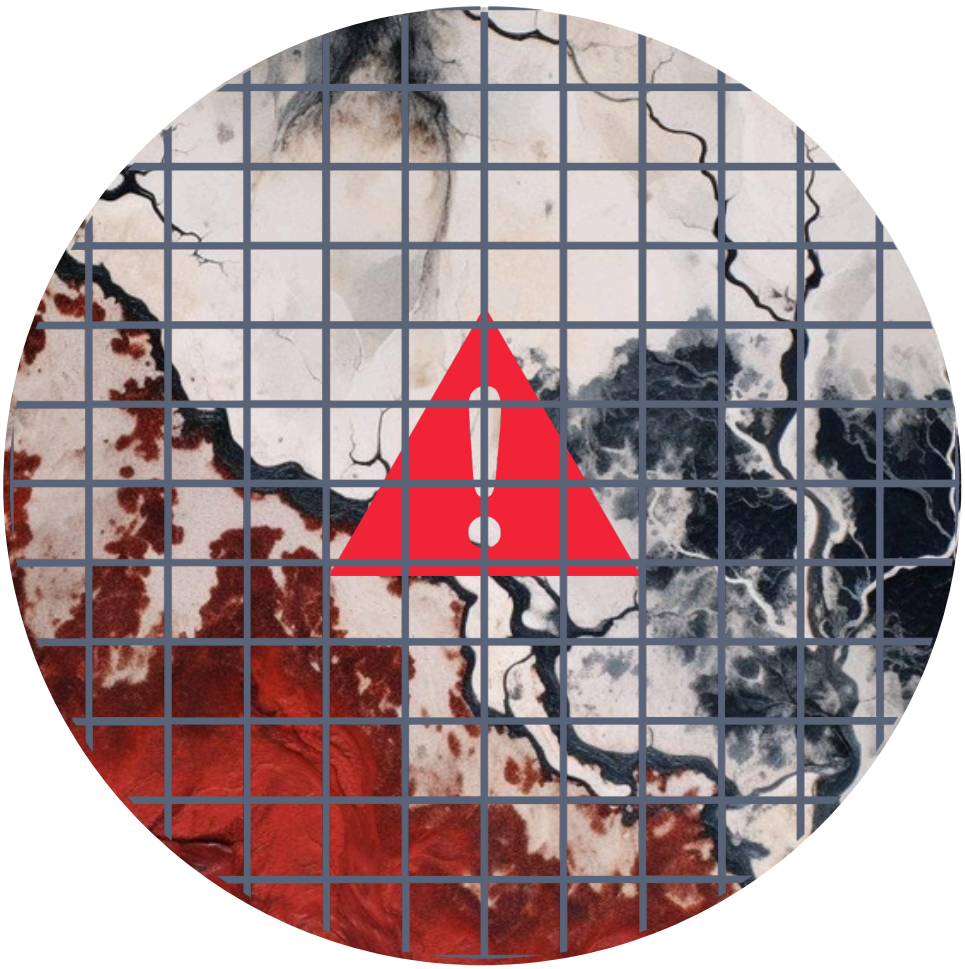
ENTHEC

WHITEPAPER

TOP 10 NETWORK VULNERABILITIES

Identify and prevent



INDEX

© 2023 Enthec Solutions. All rights reserved.

INTRODUCTION

Organizations use a large amount of resources to protect their security perimeter and prevent the entry of attacks and information leakage. Their objective is to have control over what happens within the organization to detect irregular situations, neutralize them and minimize their effects. Corporate cyber protection systems and teams have been refined and modernized in recent years, using new technologies such as artificial intelligence or machine learning to protect this security perimeter.

However, during this same period, successful cyberattacks have not only not decreased, but have increased alarmingly. The success of these attacks lies in the amount of information about the attacked organization that cybercriminals have, which makes it easier for them to prepare an attack that is very difficult to neutralize.

•What is failing in the protection of the security perimeter of organizations?
•How and where do cyber attackers access all this corporate information?

In the following document we will analyze the ten most common corporate security vulnerabilities that can be found on the Internet and that are exploited by cybercriminals to plan their successful attack. We will also discover why securing the perimeter of organizations but not controlling what is outside them compromises the security of all their systems.

© 2023 Enthec Solutions. All rights reserved.

TOP 10 VULNERABILITIES

1. CREDENTIAL LEAK

Although the protection of credentials is a priority in any organization, the leak of the same remains one of the most common vulnerabilities that wecan find in the network, especially in recent times.

Credentials are the key to entry into systems. With access to a single corporate account credential, cybercriminals can take control, move undetected within the organization's system, and gain access to confidential and sensitive information, intellectual property, or funds.

Although credential protection is a priority for any organization, credential leakage remains one of the most common vulnerabilities we can find on the network, especially in recent times when hybrid work, often implemented urgently, has caused an alarming increase in this type of leak. Normally, organizations use protocols that require passwords to be changed periodically to prevent an undetected credential leak from having serious consequences, since, thanks to these actions, the lists of leaked credentials cease to be valid in a very short period of time. This can make it difficult, to a certain extent, to achieve the first objective of credential theft: taking control of an account of a very specific profile of the organization, such as the CEO, CISO, CFO or senior board executives.

According to the Arctic Wolf report, in 2022 an organization had on average around 17 lists of corporate credentials available on the Dark Web, waiting to be used by any interested cybercriminal.

© 2023 Enthec Solutions. All rights reserved.

TOP 10 VULNERABILITIES

1. CREDENTIAL LEAK

Constant and routine password updates often lead users to acquire patterns that allow them to remember each new credential effortlessly to avoid recording it in places that could be exposed. These passwords do not always use the same word because authentication systems would not consider it valid, and that is why what is usually repeated is the pattern to choose the words, numbers, and symbols for each new password. A password leak can give a cybercriminal the keys to the pattern used by a certain user, so that he can deduce what the next updates of some of the corporate passwords will consist of and have a long-term key to the organization's system without needing anything else.

Also, credential leakage enables the cybercriminal to study the user's habits, hobbies and routines during the time that the password is valid, so that later, when designing the cyberattack, it will be easier for him to get the user to perform some type of action, such as downloading a file that he cannot suspect, to introduce ransomware into the corporate system. Therefore, credential leakage not only poses a risk in terms of control of the most relevant corporate accounts, but also because of the number of attack options it offers the cybercriminal.

Actions to be taken

Monitor what corporate credentials are available for anyone who wants to find them in the Web, Deep Web and Dark Web to take proactive protection measures that neutralize their fraudulent use to carry out an attack against the organization.

Establish periodic update protocols

Raise awareness and train users in security in order to make them aware of their own update patterns and the need to avoid them

© 2023 Enthec Solutions. All rights reserved.

TOP 10 VULNERABILITIES

2. SUBDOMAINS

An abandoned subdomain is a gateway to a cyber attack and also, a source of valuable information for a cybercriminal.

Throughout its development, an organization creates a large number of subdomains for parallel products, temporary products, advertising campaigns, marketing campaigns... Any normal activity in a company involves creating a subdomain with a website behind it, which is public for as long as the organization needs it.

Many of these subdomains are active for the duration of the operation for which they were created and then simply abandoned. The first problem resulting from this abandonment is the passage of time: people working in an organization today do not have the ability to know which subdomains were used and then abandoned in earlier stages. In addition, in small and medium-sized organizations, it is often the case that there is no professional figure dedicated to the centralized management of these subdomains, so that each one is managed by the department that activated it. In larger organizations, the existence of offices in different countries makes such centralized management of subdomains difficult.

All of these factors influence the fact that within the corporate security culture, abandoned subdomains are not perceived in most cases as a vulnerability, and a considerable number of organizations are not even aware of their existence.

© 2023 Enthec Solutions. All rights reserved.

TOP 10 VULNERABILITIES

2. SUBDOMAINS

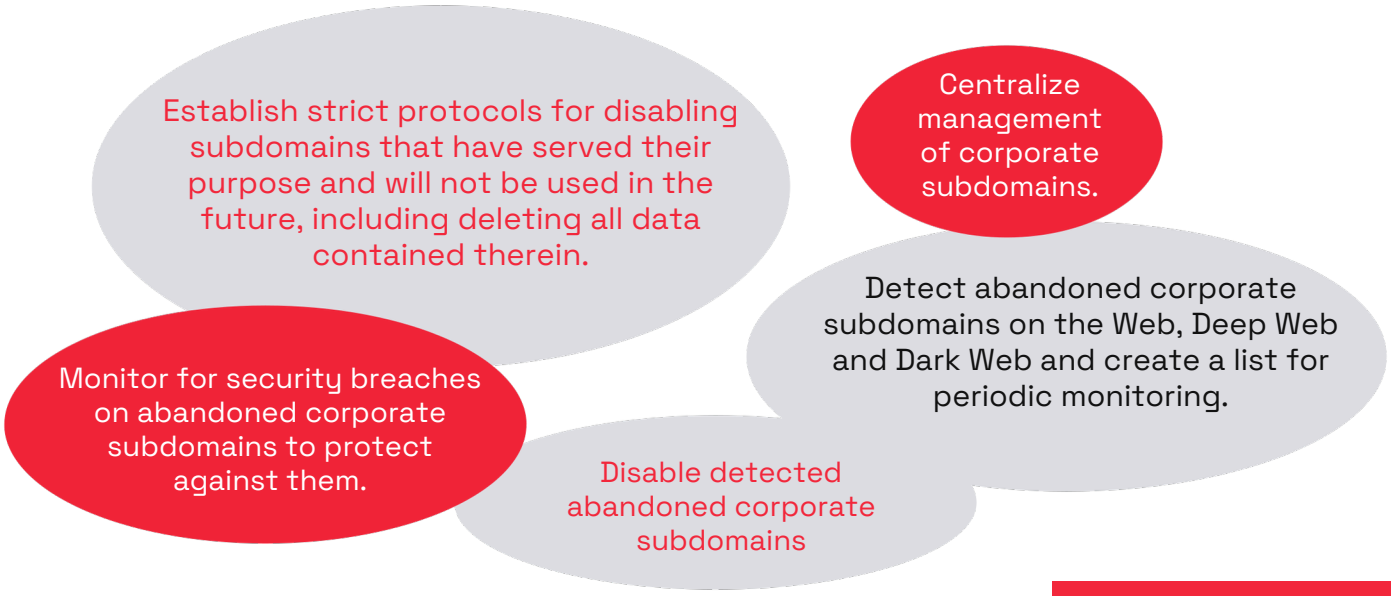
Security breaches

- **Lack of updates:** The first security breach of an abandoned subdomain is caused by the fact that it is no longer updated when it is no longer used. Therefore, no more extended protection solutions are being developed to neutralize the new forms of cyberattacks that are emerging. An abandoned subdomain that is no longer updated is the gateway to an organization's system.

- **Abandoned integration:** The most frequent process of abandonment of corporate subdomains targeting a service with third-party integrations is the inactivation of the service, but not of the subdomain, which is at the mercy of being found by a cybercriminal and reactivated as a fraudulent integration from which to trigger a cyberattack.

- **Undeleted data:** An abandoned subdomain is a sensitive information container in the organization, which can be used either to design a cyber-attack against the organization or to steal its identity for cyber-scamming third parties.

Actions to be taken



© 2023 Enthec Solutions. All rights reserved.

TOP 10 VULNERABILITIES

3. REGISTRATION ON PORTALS OF DUBIOUS TRUST

Registrations on portals of dubious trust not only endanger the security of the organization by being susceptible to becoming a vector of entry for cyberattacks. The association of corporate assets to some of these portals can pose a danger to the reputation of the organization or become nformation with which to negotiate in exchange for its non-disclosure.

All organizations have established express prohibitions on using corporate email for purposes and activities unrelated to corporate activity and business, many of which have sanctions for non-compliance.

The registration of corporate email addresses on pages of dubious reputation and security is a vulnerability of the past that has been overcome by the awareness of people who work in organizations. However, reality is different. The law protects employees' private use of corporate technological devices and establishes criteria of adequacy and reliable communication for the inclusions, prohibitions, and exclusions of activities within it.

Hybrid work and mobile corporate technological devices cause the border between work use and private use to blur and are used for registrations and visits to portals of dubious trust. The personal use of these devices is also protected by the worker's right to privacy so that not always, and in all cases, organizations can control the activity history of said devices.

In addition, statistics from adult content portals show that, during the week, after the night time, the next time slot with the most visits is during working hours.

© 2023 Enthec Solutions. All rights reserved.

TOP 10 VULNERABILITIES

3. REGISTRATION ON PORTALS OF DUBIOUS TRUST

Actions to be taken

Continuously use the means that the law allows organizations to monitor the network activity of corporate devices, without in any case undermining the right to privacy of the workers who operate them.

Periodically train and raise awareness among the organization's employees about cybersecurity and protection and action measures.

Detecting the records with domains corporates that exist in portals of dubious reputation for their control and cancellation

© 2023 Enthec Solutions. All rights reserved.

TOP 10 VULNERABILITIES

4. OUTDATED CMS

For a cybercriminal, finding a vulnerability in the CMS code means finding the entrance vector to a large number of sites, and that is why they are always in their crosshairs. An outdated CMS is a gateway to an organization's server and infrastructure.

Around 90% of the sites that have suffered cyberattacks are created with CMS, and many web pages are hacked daily in the world. Sending spam campaigns through the corporate server or stealing user data from the organization's website are some of the consequences of a CMS not being adequately maintained. Aware of being a permanent target for cybercrime, CMS providers are constantly patching their security. Therefore, automating CMS updates is the first step in addressing the maintenance of corporate CMSs.

Associated with the CMS are third-party or proprietary plugins that allow expanding CMS features and design-oriented themes. An organization can have automated updates for the CMS, but not for some plugins, and it may even occur that if some plugins are too old and no longer used by the organization, they may even be abandoned or outdated.

According to data provided by the firm W3Techs, in 2020 WordPress became the open source content management system that supports 40% of the websites on the Internet. If we add to this figure those of the rest of the most popular CMS, we can understand its influence on the cybersecurity of organizations.

© 2023 Enthec Solutions. All rights reserved.

TOP 10 VULNERABILITIES

4. OUTDATED CMS

Actions to be taken

When installing third-party plugins, assess the trajectory of the author, the degree of compatibility of the plugin with the CMS, the maturity of the code and its reputation

Audit the CMS, control its maintenance status and that of installed plugins.

Always keep the update of the CMS and installed plugins automated

© 2023 Enthec Solutions. All rights reserved.

TOP 10 VULNERABILITIES

5. EXPOSED DATABASES

Many of the exposed databases are discovered by network researchers, and the affected organizations only become aware of the flaws in their database configuration once they are notified.

The database is one of the most valuable assets of any organization. Its protection is a priority for any company's security systems. However, both the smallest and largest organizations regularly suffer security breaches that leave their databases exposed from the moment they occur until the moment they are detected, which is usually not immediate.

The search results for "exposed databases" or examples of organisations with sensitive data, such as Medicall, a healthcare company – with an exposed database containing 2.7 million private recordings of Swedish patients* – or as popular as Adobe – an unauthenticated database exposed and detected in 2019 by the company Comparitech** – show that database exposure is a frequent and recurring problem affecting all types of organisations.

A corporate database can be exposed after a cyber attack, but also due to poor configuration or lack of maintenance and updates to the database itself.

Initially, databases were hosted in on-premise solutions, but since the development of cloud computing and the widespread use of hybrid or third-party clouds, the protection of corporate databases has become more complex, since security, in many cases, is no longer entirely in the hands of the organization itself.

It is just as common for databases to be exposed as a result of crime or negligence on the part of the organization or the people who work there.

© 2023 Enthec Solutions. All rights reserved.

TOP 10 VULNERABILITIES

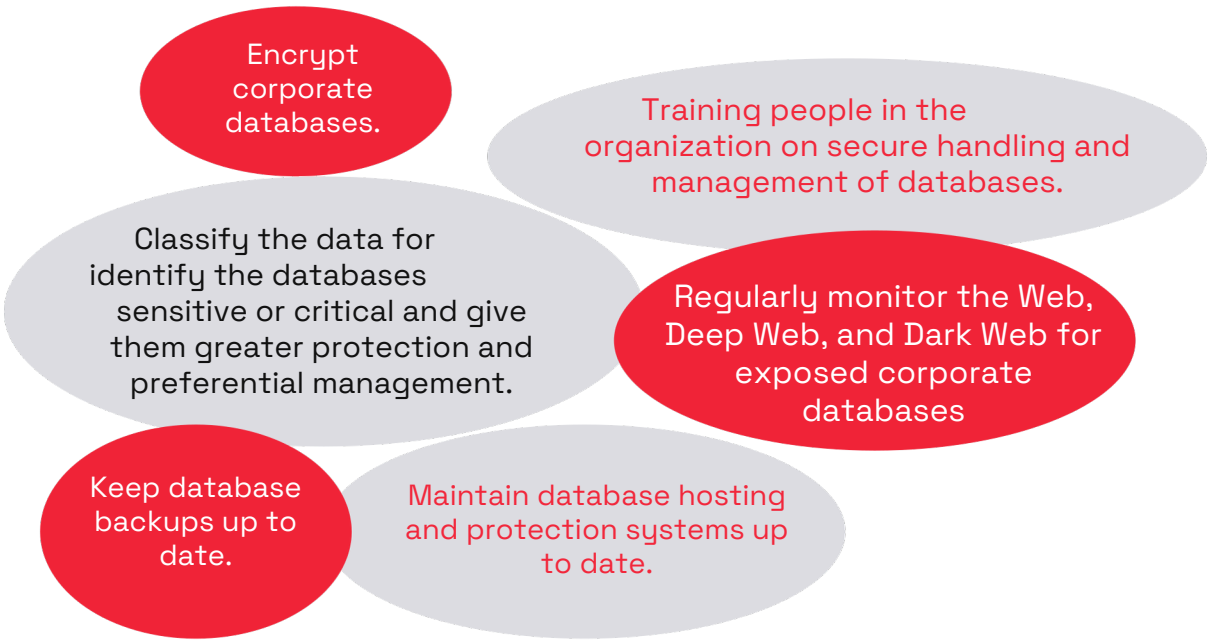
5. EXPOSED DATABASES

Security breaches

An exposed database poses multiple risks to an organization:

- The organization fails to comply with its duty to protect data containing thirdparty sensitive information.
- Corporate data are at the disposal of anyone who finds them to be used for any purpose.
- Corporate data may be deleted by anyone who finds them, and corporate information for which there is no copy of security can disappear.
- The organization faces a reputational crisis.

Actions to be taken



© 2023 Enthec Solutions. All rights reserved.

6. DOCUMENTATION PROTECTED BY THE GDPR

Any organization document, no matter how small, that contains data from third-parties collected by it and that is leaked or exposed can cause a lawsuit by the third-party affected and an administrative sanction.

This vulnerability shares characteristics with the previous one involving the exposure of databases; sometimes it is even a consequence of it, although not always.

The amount of personal and sensitive data of third parties, clients, partners, suppliers, that organizations collect daily has made their protection, based on the right to privacy, a priority for States and legislators. All organizations, regardless of their size, that collect data from third parties are obliged to protect them in the manner and to the extent established by the General Data Protection Regulation (RGPD 2016/679), which includes the corresponding sanctions for the wilful or negligent failure to comply with said protection.

The obligation to protect and monitor third-party data is, therefore, a task for each and every person who works in the organization and handles data of this type in any of the corporate tools: a simple email that transfers confidential data of a third party covered by the GDPR may constitute an infringement against it.

Since the entry into force of the European Union's NIS 2 Directive, the directors of the organizations obliged by its articles are personally liable in the event that it is proven that the organization has not taken sufficient and diligent measures to protect third-party data covered by the GDPR.

© 2023 Enthec Solutions. All rights reserved.

TOP 10 VULNERABILITIES

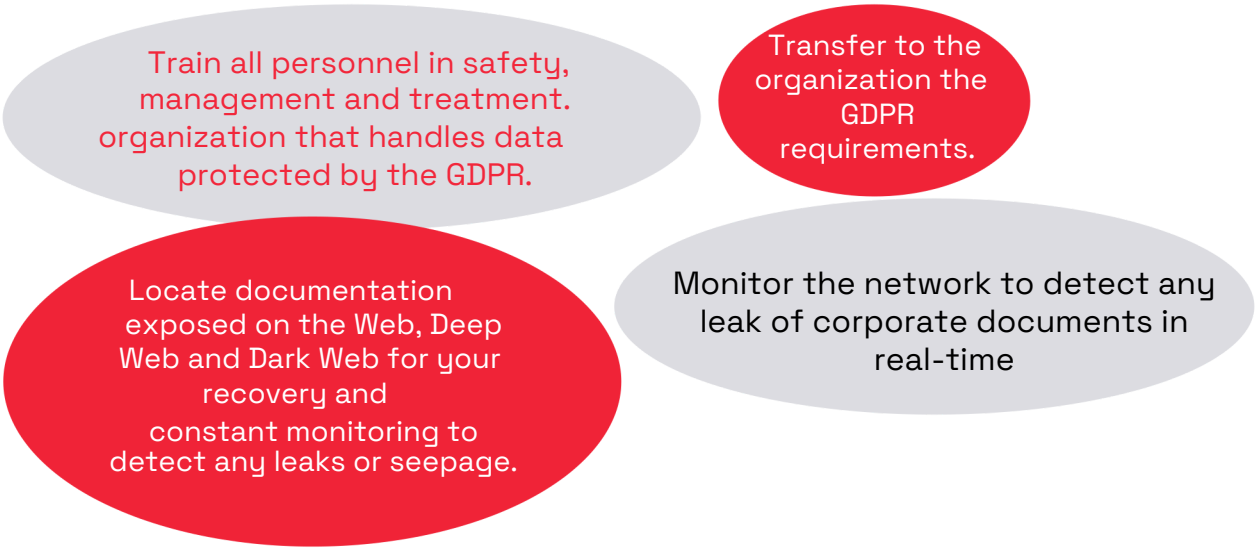
6. DOCUMENTATION PROTECTED BY THE GDPR

Security breaches

As with the exposure of databases, the exposure of documentation in violation of the GDPR is a vulnerability that has multiple consequences for the organization:

- Administrative sanctions and compensation to affected third parties.
- Corporate reputation crisis.
- Organization's responsibility for fraudulent use of data protected by third parties.

Actions to be taken



© 2023 Enthec Solutions. All rights reserved.

TOP 10 VULNERABILITIES

7. SENSITIVE OR CRITICAL INFORMATION

The seriousness of the exposure of this documentation depends on its content, but, in any case, the reputation of the organization that does not have the privacy of its internal documentation well controlled is always at stake.

In addition to the exposure of databases or documentation with data protected by the GDPR, the exposure of documentation with sensitive or critical information, current or past, of the organization is another frequent vulnerability in the network and which can also cause a multiple risk when detected by cybercriminals.

Contracts, negotiations, strategies, market studies, competitor studies... the amount of documentation exposed by organizations on the Web, Deep Web and Dark Web is immense. Cybercriminals use the information provided by these types of documents in different ways, depending on the relevance of the information they contain: they can ask for a ransom for it or a payment for not disclosing it, they can sell it to interested competitors, they can use it to gather information to plan an attack or all of the above. Few organizations are aware of the risks that can be created in a chain from a single leaked corporate document in the hands of someone who knows how to use it.

Actions to be taken

Locate internal documents exposed on the Web, Deep Web and Dark Web to recover them and neutralize the possible consequences of its illegal use.

Monitor the network to detect any corporate information leaks in real time.

Establish a corporate culture of preparation, handling, management and safe storage of all internal documentation

© 2023 Enthec Solutions. All rights reserved.

TOP 10 VULNERABILITIES

8. SOURCE CODE

The source code can be leaked in many ways, intentionally or not, both through the activity of people in the organization, third parties from external services that collaborate in the development of software or as a result of a cyber attack.

Source code is part of an organization's intellectual property, a valuable asset that does not always receive adequate protection for its importance.

In theory, corporate source code should be handled, treated and shared with the highest security standards, as the information it contains is critical intellectual property and vital to the competitive position of the organization. In practice, the speed with which source code creation is required for organizations means that programmers cannot always be strict when it comes to handling source code. DevOps tools have been developed with the aim of streamlining these times, which contributes to source code security.

However, to implement them, an organization must first migrate all its systems and legacy to a fully cauterized cloud environment, which complicates the process and delays adoption.

When a company's source code is exposed and detected by a cybercriminal, it can end up in the hands of competitors who will have a guide to copy the corporate solution, it can be used to clone the solution and scam on behalf of the organization, or it can be used to scam the organization directly. With the source code, the cybercriminal will know what the organization's programming practices are, if there are static analyses, security levels, code optimization, and will be able to quickly find out the quality of work and the level of protection of that organization.

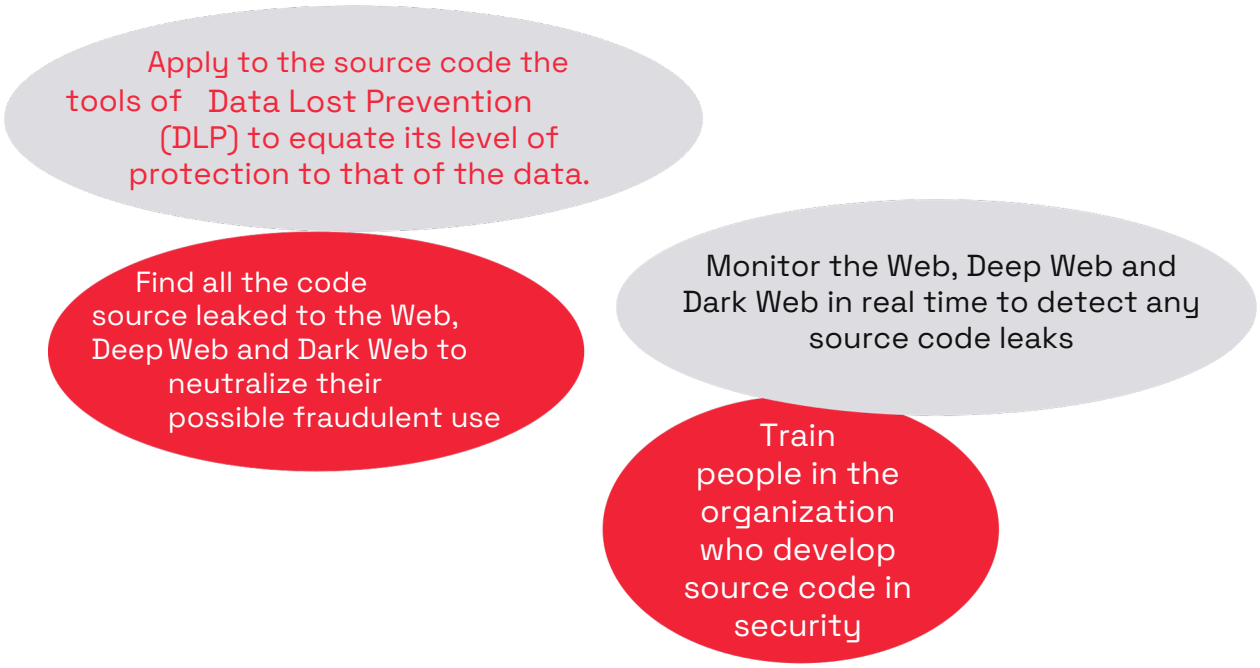
Publicizing the source code leaves it open to being modified by anyone who has an interest in it. The malware association with the PDF format is due to the fact that Adobe's source code was exposed on the Internet without any control for a long time.

© 2023 Enthec Solutions. All rights reserved.

TOP 10 VULNERABILITIES

8. SOURCE CODE

Actions to be taken



© 2023 Enthec Solutions. All rights reserved.

TOP 10 VULNERABILITIES

9. PROJECT MANAGEMENT

Leaks of information contained in project management tools mean that all the work of any department in the organization is available to whoever finds it in a web, deep web or dark web crawl.

Organizations use project management tools across all departments to enable teams to organize and share work quickly and effectively. Some of these project management tools are installed within the organization's system, so they can be a gateway to the organization's system if they are not protected.

When information contained in project management tools is leaked, there is a multiple risk, because not only can this information be used to plan a cyber attack or to demand ransoms, but it can also be sold to competitors or used to cause a reputation crisis for the organization. Added to all this is the impossibility of guaranteeing the integrity of the project, since anyone who has access to it through the management tool can maliciously modify its terms at any time.

In the case of projects carried out in collaboration with third parties, it is just as important for the organization to guarantee their protection and confidentiality as it is to be sure that the collaborators do the same under the same terms.
Actions to be taken

Locate internal documents exposed on the Web, Deep Web and Dark Web to recover them and neutralize the possible consequences of its illegal use.

Monitor the network to detect any corporate information leaks in real time.

Establish a corporate culture of preparation, handling, management and safe storage of all internal documentation

© 2023 Enthec Solutions. All rights reserved.

TOP 10 VULNERABILITIES

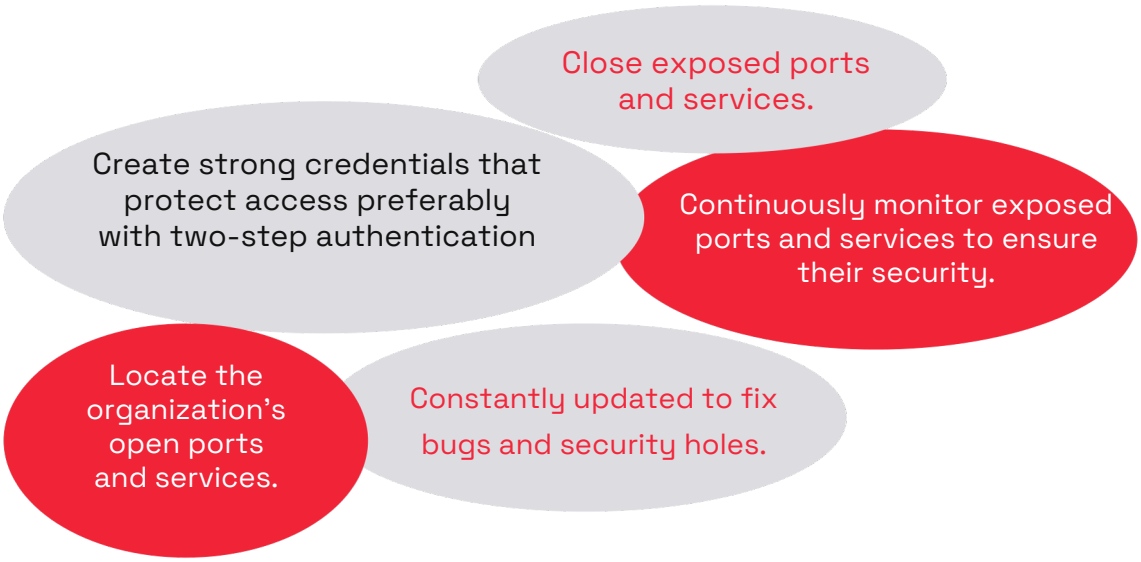
10. EXPOSED SERVICES

An open and exposed service constitutes a high risk for organizations, since all the information that passes through them is transmitted without encryption.

It is not difficult for a cybercriminal to find file sharing services or connection services on the Internet whose ports are open.
The security of a port depends, above all, on its management and the use to which it is put. The service that generates or consumes the traffic that passes through a particular port must be updated to incorporate patches for security breaches that may appear, either due to configuration errors or due to adaptation to new technologies that are emerging.

An unpatched FTP port is a corporate security risk that can be exploited by cybercriminals to validate anonymous authentications or as an entryway for malware. An unencrypted service can enable an unauthenticated attacker to execute remote processes. Unsecured ports and protocols can reveal to attackers a lot of information about your infrastructure, servers, and the organizations that are using them, such as network shares.

Actions to be taken



© 2023 Enthec Solutions. All rights reserved.

ENTHEC

WHITEPAPER

kartos©

Kartos Corporate Threat Watchbots: Continuous Threat Exposure Management (CTEM)

Automated, continuous, real-time monitoring of the organization's threat exposure, focused on cybersecurity and business criteria.

EXTERNAL ATTACK SURFACE

Location of the Company's open and exposed information and vulnerabilities on the Internet, the Deep Web, Dark Web and Social Networks: Phishing, fraud and scam campaigns; CVEs; DNS health; leaked passwords and credentials; leaked and exposed documentation and databases.

DIGITAL RISK PROTECTION

Detection of contextual information about potential attackers, their tactics and processes for carrying out malicious activities. Elimination of malicious activities on behalf of the Company. Brand, domain and subdomain protection. Corporate email protection. Ransomware protection. Web security and threat removal.

THIRD PARTY RISK

Real-time monitoring of third-party risk. Objective data on ongoing threats related to the value chain. Comprehensive view of any organization's cybersecurity maturity using a non-intrusive, external approach. Extension and weighting of information provided by traditional third-party risk assessment methods.

COMPLIANCE

Monitoring of corporate and third-party legal compliance based on objective data taken in real time.
ISO 27001. PCI - DSS. ENS. RGPD.
Justification of compliance with legal and regulatory requirements for associations, mergers and acquisitions, audits, certifications and contracts with the administration

CYBERSECURITY SCORING

Enables security information to leave the CISO's office and be easily presented to people who need to be involved in security management without technical training. Own and third-party cybersecurity scoring for partnerships, audits, mergers, acquisitions, and government contracts.

Analysis of 9 threat categories

- **Network**
- **DNS Health / Phishing**
- **Patch Management**
- **IP Reputation**
- **Web Security**
- **Email Security**
- **Document Filtering**
- **Credential Filtering**
- **Social Networks**

ENTHEC

WHITEPAPER

kartos©

AI layer that enables 100% automated operation without human intervention anywhere of the process.

Strictly non-intrusive tool.
The research is carried out on the Internet, the Deep Web and the DarkWeb and the IT perimeter of the organizations is not attacked, so its operation and the information obtained strictly comply with the imposed limits.
by legislation.

The only platform that analyzes **conversations on social networks from the threat and attack detection perspective,** beyond the relating to reputation and branding.

Continuous operation 365x24x7, allowing detection of leaks of new information practically in real time.
real time.

Maximum ease of use. Does not require no complex configuration. Simply enter the domain into the platform and it works autonomously, without the need to configure search parameters or any other information location criteria.

Automated, objective and continuous monitoring of the risks caused by third parties belonging to the External Attack Surface of the organization.

Learn more about our licenses.
Try our tool for free.
Get started with Kartos and find and mitigate your vulnerabilities.

hello@enthec.com

Enthec Solutions is a Spanish technology company that develops cybersecurity software for the protection of organizations and people. Enthec Solutions has established itself as one of the Deep Tech companies with the most innovative and effective Cyber surveillance solutions thanks to the success of its **Kartos Corporate Threat Watchbots** platform, which provides organizations with Cyber Security, Cyber Intelligence, Cyberscoring, Compliance and Third-Party Risk Management Capabilities, and its innovative **Qondar Personal Threat Watchbots** platform for the individual online protection of the organization's relevant people.

www.enthec.com

© 2025 Enthec Solutions. All rights reserved.