ENTHEC

WHITEPAPER

TOP 10 NETWORK VULNERABILITIES

Identify and prevent

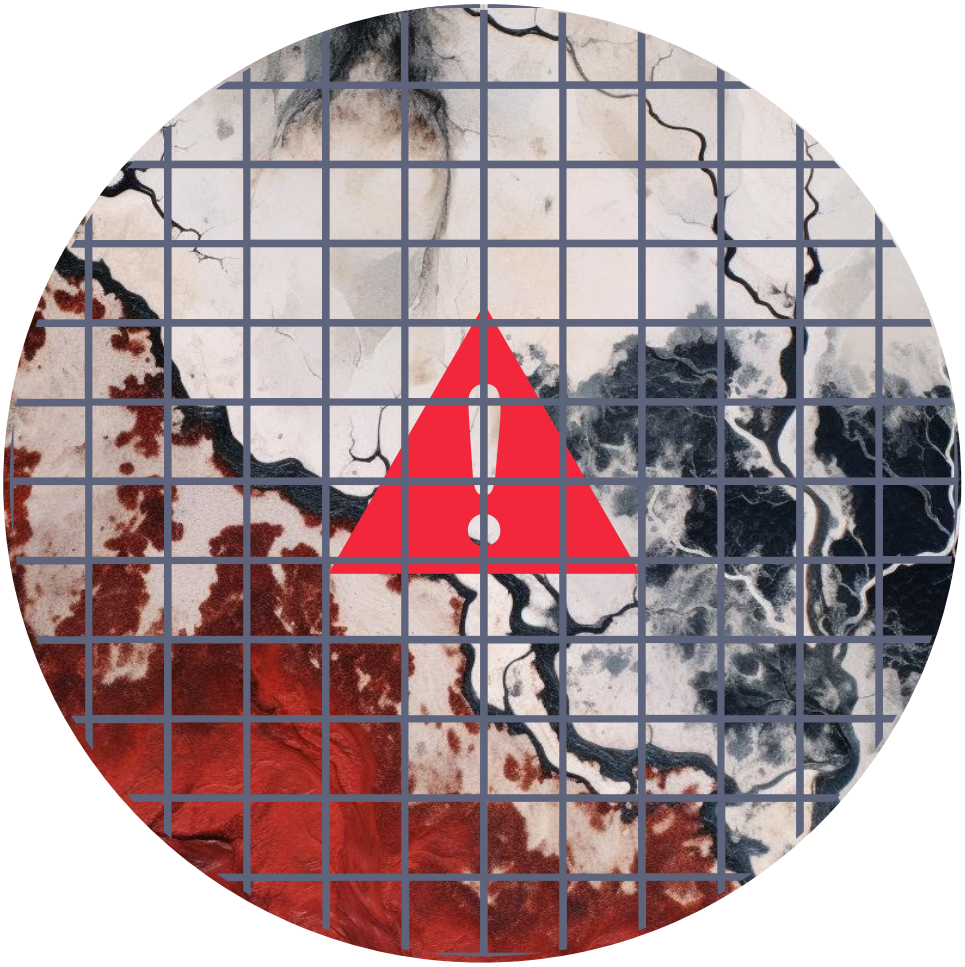


TABLE OF CONTENT

INTRODUCTION

Organizations use a lot of resources to protect their security perimeter and prevent attacks and information leakage. Their objective is to keep under control what is happening inside the organization to detect irregular situations, neutralize them and minimize their effects. In recent years, corporate cyber-protection systems and equipment have been perfected and modernized, using new technologies such as artificial intelligence or machine learning to protect this security perimeter.

However, at the same time, successful cyberattacks have not decreased, but they have increased alarmingly.

The success of these attacks lies in the amount of information about the targeted organisation that cybercriminals have at their disposal, which makes it easier for them to prepare an attack that is very difficult to neutralize.

- What is going wrong in protecting the security perimeter of organizations?
- How and where do cyber attackers gain access to all this corporate information?

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

TOP 10 VULNERABILITIES

1. CREDENTIALS 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 we can find in the network, especially in recent times.

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

Even though credential protection is a priority in any organization, credential leakage continues to be one of the most common vulnerabilities that we can find on the web, especially in recent times when hybrid work, and in many cases implemented urgently, has caused an alarming increase in this type of leak. Typically, organizations use protocols that force passwords to be changed every so often to prevent an undetected credential leak from having severe consequences since, thanks to these actions, the lists of leaked credentials become invalid quickly. This can make it somewhat more challenging to achieve the first objective of credential theft: taking control of an account of a particular profile of the organization, such as the CEO, CISO, CFO, or managers of the main board.

According to an Artic Wolf report, in 2020, an organization had an average of 17 corporate credential lists available on the Dark Web, waiting for any interested cybercriminal to use them.

TOP 10 VULNERABILITIES

1. CREDENTIALS LEAK

The constant and routine updating of passwords often causes users to acquire patterns that allow them to remember each new credential effortlessly to avoid having to record it in places where it could be exposed. These passwords do not always use the same word because the authentication systems would not consider it valid, and for this reason, what is usually repeated is the pattern to choose the words, figures, and symbols of each new password. A password leak can give a cybercriminal the passwords of the pattern used by a particular user so that they can deduce what the next updates of some of the corporate passwords will consist of and have a long-term access key to the organization's security system without needing anything else.

Also, leaking credentials empowers the cybercriminal to study the user's habits, hobbies, and routines when the password is valid so that later, when designing the cyberattack, it will be easier for him to get him to perform some action, such as downloading an unsuspected file to introduce ransomware to the corporate system...

Therefore, the leaking of credentials 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 take

Monitor what corporate credentials are available to anyone who wants to find them on 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

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

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, etc. Any regular activity in a company involves creating a subdomain with a web page 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 abandoned. The first problem derived from this abandonment is the passage of time: people who work in an organization today cannot know which subdomains were used and abandoned in previous stages. In addition, in small and medium-sized organizations, there is often no professional figure dedicated to the centralized management of these subdomains, so each one is managed by the department that activated it. In larger organizations, headquarters in different countries make such centralized management of subdomains difficult.

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

TOP 10 VULNERABILITIES

2. SUBDOMAINS

Security breaches

- **Lack of updates:** The first security breach of an abandoned subdomain is caused by the fact that, when it is no longer used, it is also no longer updated, and therefore, there are no more extended protection solutions that 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 take

Establish strict protocols for disabling subdomains that have fulfilled their function and will not be used in the future, including the deletion of all the data included in them.

Centralize the management of corporate subdomains

Detect abandoned corporate subdomains on the Web, Deep Web and Dark Web and create a list for periodic control

Monitor security breaches of abandoned corporate subdomains to protect against them

TOP 10 VULNERABILITIES

3. REGISTRATION IN UNRELIABLE PORTALS

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 information 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 on weekdays, the next most visited time slot after night time is during working hours.

TOP 10 VULNERABILITIES

3. REGISTRATION IN UNRELIABLE PORTALS

Actions to take

Continuously use the means that the law allows organizations to control the activity on the network of corporate devices, without in any way undermining the right to privacy of the workers who operate with them

Periodicaly train and raise awareness among the organization's workers about cybersecurity and protection and action measures.

Detect registrations with corporate domains that exist in portals of dubious reputation for their control and cancellation

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 network. If those of the rest of the most popular CMS are added to this figure, their influence on organizations' cybersecurity can be understood.

TOP 10 VULNERABILITIES

4. OUTDATED CMS

Actions to take

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 the installed plugins

Always keep the update of the CMS and installed plugins automated

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.

Databases are one of the most valuable assets of any organization. Protecting those assets is a priority of any company's security systems. However, from the smallest to the most prominent, organizations routinely suffer security breaches that expose their databases from when they occur to when they are detected, usually not immediately.

The search results for "exposed databases" or examples of organizations with sensitive data, such as Medical, dedicated to healthcare - 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** - demonstrate that database exposure is a frequent and recurring problem affecting all types of or organizations.

A corporate database may be exposed after a cyberattack but also because of a misconfiguration or lack of maintenance or updates to the database itself.

It is just as frequent that the exposure of the databases is the result of a crime as the result of negligence on the part of the organization or the people who work for it.

TOP 10 VULNERABILITIES

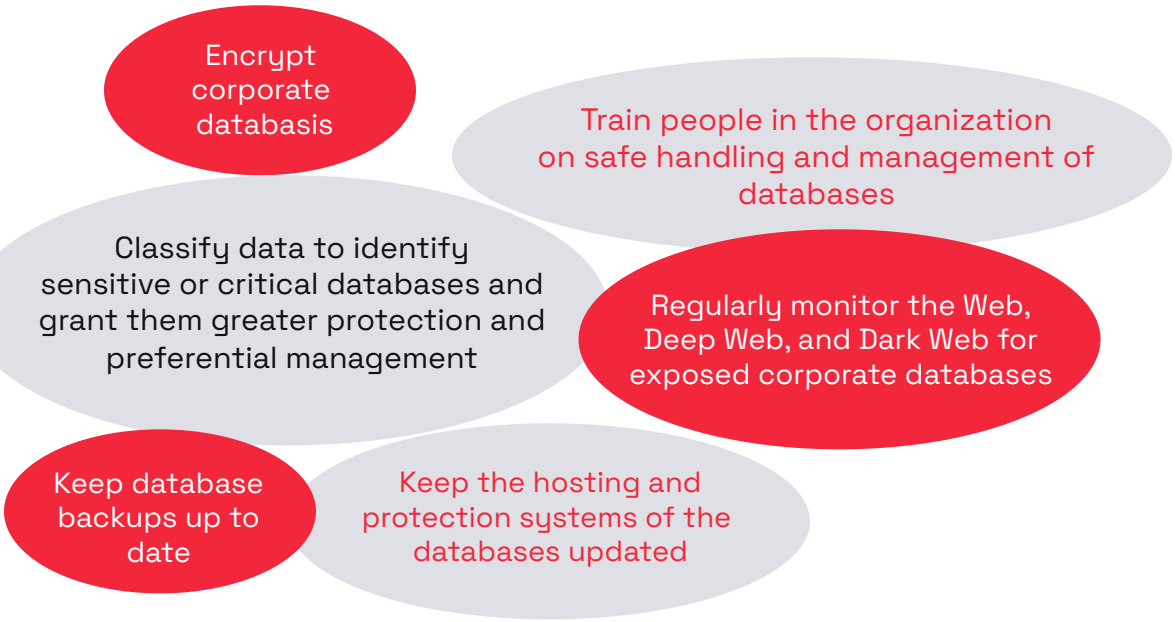
5. EXPOSED DATABASES

Security breaches

An exposed database poses multiple risks to an organization:

- The organization fails to comply with its duty to protect data containing third-party 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 reputation crisis.

Actions to take



TOP 10 VULNERABILITIES

6. DOCUMENTATION PROTECTED BY DATA LAW

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 vulnerability of database exposure and is sometimes, but not always, a consequence.

The amount of personal and sensitive data of third parties, customers, partners, and suppliers that organizations collect daily has made their protection, based on the right to privacy, a priority for States and legislators.

Every organization, regardless of size that collects data from third parties is obliged to protect such data in the manner and to the extent set out in laws like the European General Data Protection Regulation (GDPR 2016/679), which includes penalties for wilful or culpable breach of such protection.

The obligation to protect and monitor the data of third parties is, therefore, a task for every person working in the organization and handling data of this type in any of the corporate tools: a simple e-mail transferring confidential data of third parties covered by the law may constitute an infringement of it.

It is important to note that any document of the organization, however small, containing third-party data collected by the organization that is leaked or exposed may be subject to legal action by the injured third party and administrative penalties.

TOP 10 VULNERABILITIES

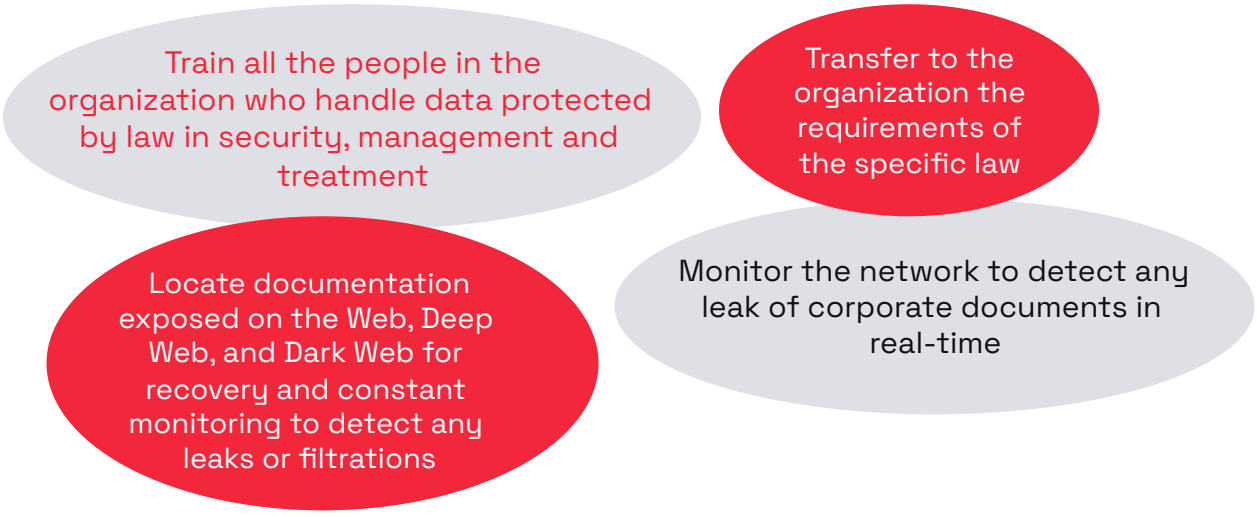
6. DOCUMENTATION PROTECTED BY DATA LAW

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 penalties and compensation to affected third parties.
- Corporate reputation crisis.
- Liability of the organization for fraudulent use of third-party protected data.

Actions to take



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 law, the exposure of documentation with the organization's sensitive or critical information, current or past, is another frequent vulnerability on the network that can also cause multiple risks when detected by cyber criminals.

Contracts, negotiations, strategies, market studies, competitor studies... There is an immense amount of exposed documentation of organizations on the Web, the Deep Web, and the Dark Web.

Cybercriminals use the information provided by those documents in different ways, depending on the relevance of the information they contain: they may ask for a ransom or payment for non-disclosure, they may sell it to interested competitors, they may use it to gather information to plan an attack, or all of these together. Few organizations know the cascading risks triggered by a single leaked corporate document in the hands of someone who knows how to use it.

Actions to take

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

Monitor the network to detect any leak of corporate information in real time

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

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.

The source code is part of an organization's intellectual property, a valuable asset not always protected. Theoretically, a corporate source code should be handled, treated, and shared with the highest security standards because its information is critical intellectual property vital to the organization's competitive position.

In practice, the speed needed to generate a source code for organizations means that programmers cannot always be strict in treating the source code.

DevOps tools have been developed to streamline these times, contributing to the source code's security. However, to implement them, an organization must first migrate all the systems and legacy to a clustered platform cloud environment, complicating the process and delaying adoption.

When a company's source code is exposed and detected by a cybercriminal, it may end up in the hands of a competitor, 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 itself directly. With the source code, the cybercriminal will know about the organization's programming practices, if there are static analyses, security levels, and code optimization, and will also be able to quickly find out the quality of work and the level of protection of that organization.

The publicity of the source code leaves it open to be transformed by anyone interested in it.
The association of malware to the PDF format is because Adobe's source code was exposed on the network for a long time without any control.

TOP 10 VULNERABILITIES

8. SOURCE CODE

Actions to take

Apply the Data Loss Prevention (DLP) tools to the source code to assimilate its level of protection to that of the data.

Locate all leaked source code to the Web, Deep Web and Dark Web to neutralize its possible fraudulent use

Monitor the Web, Deep Web, and Dark Web in real-time to detect any source code leaks

Train people in the organization who develop source code in security

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 in all departments to enable teams to organize and share work immediately and effectively. Some of these project management tools are installed within the organization's system and can be a gateway into the organization if they are not protected.

Leaks of the information contained in project management tools mean that all the work carried out in any department in the organization - marketing, finance, IT, projects, credentials, market analysis, and decisions, etc. - is available to anyone who finds it in a crawl of the Web, the Deep Web or the Dark Web.

As in the cases we have analyzed above, there are multiple risks because this information can not only be used to plan a cyber-attack or to demand ransom but can also be sold to competitors or used to provoke a reputational crisis for the organization. On top of this, the project's integrity cannot be guaranteed, as anyone who has access to it through the management tool can maliciously change its terms at any time.

In the case of projects carried out in collaboration with third parties, it is just as crucial for the organization to guarantee its protection and confidentiality as it is to ensure that its collaborators do the same on the same terms.

Actions to take

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

Monitor the network to detect any leak of corporate information in real-time

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

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.

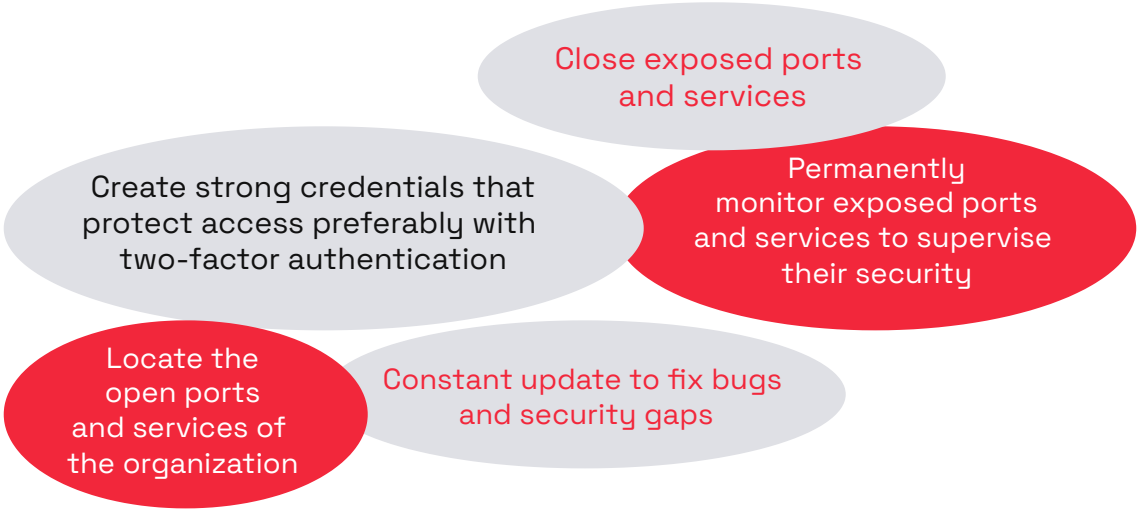
It is easy for a cybercriminal to find file-sharing or connection services on the Network with open ports.

An open and exposed service constitutes a high risk for organizations, as all information passing through them is transmitted unencrypted.

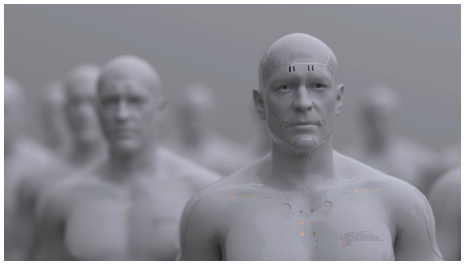
The security of a port depends, above all, on its management and use. The service that generates or consumes the traffic through a given port must be updated to incorporate patches for security breaches as they appear, either due to configuration errors or to the adaptation to new technologies.

An outdated FTP port is a corporate security risk, which cybercriminals can exploit to validate anonymous authentication or as a gateway for malware. An unencrypted service may even enable an unauthenticated attacker to execute processes remotely. Unsecured ports and protocols can show attackers much information about your infrastructure, the servers, and the organizations using them, such as network shares.

Acciones to take



kartos©
XTI watchbots



An organization's cybersecurity systems know what's going on within their IT perimeter, but they do not control what is happening outside and do not know what information a cybercriminal can find on the network.

It only takes one person in the organisation to forget or lose their unprotected mobile phone for their email and access to corporate hard drives to be exposed. Or if a Trojan on a PC hacks into a USB stick, all information is immediately leaked.

That's why an organization's perimeter protection is not enough. That's why it needs to be extended beyond that perimeter.

Controlling the leakage of corporate assets and the exposure of information on the network is essential to guarantee the organization's security, minimize the possibility of cyberattacks and reputational crises, and neutralize those detected.

Kartos XTI Watchbots platform by Enthec Solutions has been developed to meet this information control need on the organization's networks. Kartos uses Artificial Intelligence to look for information just as cybercriminals do and accesses data from publicly available sources containing information available to anyone who knows how to look for it.

Kartos requires no deployment, no installations, and no access to corporate systems: its robots autonomously search the network continuously and, using AI, analyze and present the results of their crawl in a dashboard with eight vectors designed to facilitate the remediation process.

In addition to the advantages of detecting the organization's vulnerabilities through the Kartos platform, there are also the advantages of detecting those vulnerabilities in projects and activities shared with third parties. Kartos allows an organization to control the exposed corporate information, where it is found, and the risk of an attack.

Kartos XTI Watchbots enables the organization to control the most frequent vulnerabilities in the network, the corporate information that is exposed, where it is located, the risk of third parties, and the risk of suffering an attack.

ENTHEC

WHITEPAPER

kartos©

XTI watchbots

Kartos XTI Watchbots: EASM + DRPS + SRS on a single platform

Kartos XTI Watchbots is the Cyber-surveillance platform developed by Enthec Solutions to extend the security perimeter controlled by organizations and institutions. Conceived from a hacker strategy approach, Kartos is in an ongoing R&D process to incorporate categories and capabilities ahead of the evolution of cyberattacks.

External Attack Surface Management

Detection of corporate assets and information about systems, cloud services, and applications that are available and visible in the public domain to any cybercriminal.

Digital Risk Protection Services

Detection of contextual information about possible attack agents, their tactics and processes to carry out malicious activities, and removal of malicious activities on behalf of the organization.

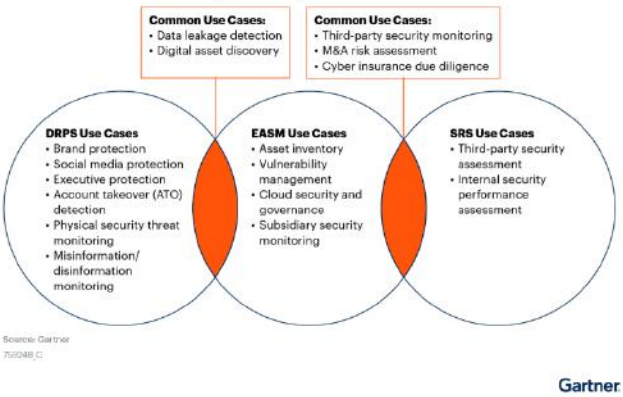
Security Rating Services

Independent risk assessment of own and third parties for a broad visualization of the maturity in cybersecurity of any organization using an external approach. Extension and weighting of information provided by third-party risk assessment traditional methods.

Analysis of 9 threat categories

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

The Common Use Cases Supported by DRPS, EASM and SRS



Gartner

ENTHEC

WHITEPAPER

kartos©

XTI watchbots

- **AI layer** that allows operation 100% automated without intervention in any part of the process.
- **Strictly non-intrusive tool.** The research is conducted on the Internet, the Deep Web and DarkWeb, and does not attack the IT perimeter of companies, so their operation and the information obtained strictly comply with the limits imposed by the legislation.
- The only platform that analyzes **conversations on social networks from the perspective of detecting threats and attacks** beyond that relating to reputation and branding.
- **Continuous operation 365x24x7,** allowing you to detect new information leaks practically in real time.
- **Maximum ease of use.** No complex configuration is required. Simply enter the domain in the platform and it works autonomously without configuring search parameters or other criteria for locating information.
- **Automated, objective, and continuous monitoring** of risks caused by third-parties belonging to the Company´s External Attack Surface.

Learn more about our licenses
Try the XTI Cyber-Intelligence for free
Start using Kartos → hello@enthec.com

Enthec is a Deep Tech that develops and manufactures cybersecurity software with a hacker approach to extend the reach of cyber-protection strategies of organizations.

Founded as a startup in 2019 by María Rojo, Enthec has grown through funding rounds and the success of its Kartos platform to consolidate itself as one of the Deep Tech with more innovative and effective solutions in the field of Cybersecurity.

To learn more about us, you can visit our website:

www.enthec.com