A Work Project presented as part of the requirements for the Award of a Master's degree in Business Analytics from the Nova School of Business and Economics.

OPTIMIZING GOSP'S VULNERABILITY MANAGEMENT THROUGH DATA VISUALIZATION

FRANCESCA FONTANESI

Work project carried out under the supervision of:

Qiwei Han

16/12/2022

Abstract: As vulnerabilities play a key role in cyber security, this paper focuses on highlighting the critical aspects that characterize these flaws and the possible phenomena that might arise as a consequence of inefficient vulnerability management. Currently, at GOSP, vulnerability management is approached manually, and the analyses performed are informative yet not relevant from a decision-making point of view. The goal of this paper is to propose a solution to mitigate GOSP's problems that mine the efficiency of a process which, by definition, must be efficient, reaching a time- and resource-optimized process.

Keywords: Business Analytics, Data Analytics, Cyber-Security, Vulnerabilities, Vulnerability Management, Data Visualization, Process Optimization.

Confidentiality Clause:

This final thesis is based on internal, confidential data and information of the following enterprise: GOSP. This work must only be made available to the first and second reviewers and authorized members of the board of examiners. Any publication and duplication of this final thesis - even partially - is strictly forbidden. An inspection of this work through third parties requires the explicit consent of both the author and GOSP.

This work used infrastructure and resources funded by Fundação para a Ciência e a Tecnologia (UID/ECO/00124/2013, UID/ECO/00124/2019 and Social Sciences DataLab, Project 22209), POR Lisboa (LISBOA-01-0145-FEDER-007722 and Social Sciences DataLab, Project 22209) and POR Norte (Social Sciences DataLab, Project 22209).

TABLE OF CONTENT

1. Introduction

As the years go by, organizations in both the public and private sectors are becoming increasingly dependent on information technology and information systems making IT become a vital and integral part of every business plan. Although the use of IT facilitates an enormous amount of processes and helps save resources, information systems are subject to possible malicious acts, also known as threats, that exploit vulnerabilities and seek to damage the information processed, stored, and transmitted by compromising its integrity, confidentiality, or availability resulting in severe effects on the organization itself. Vulnerability management, which aims at remediating vulnerabilities to reduce as much as possible the success of a cyber-attack, plays a key role in cyber security.

This paper aims at identifying a solution to the main problems affecting GOSP's vulnerability management: before, the vulnerability management process was approached manually, with the result of slowing down the whole system. Furthermore, the carried-out analyses focused merely on reporting to each legal entity's CISO and GOSP's CSO the number of vulnerabilities for each of the classifications considered, resulting in a lack of relevant observations that could help the organization's decision-making, mainly in terms of identification of the bottlenecks affecting the efficiency of the business.

To solve these problems, an automatized data curation step using business intelligence tools was introduced and a Power BI dashboard was created containing visuals that aim at guiding the user in identifying the least efficient segments of the company on which an intervention is needed and where security awareness must be increased.

Firstly, a theoretical overview of the critical aspects of security vulnerabilities is given discussing the costs deriving from a possible breach to enable the user to understand the huge

impact that these IT flaws represent for any organization and why they must be managed efficiently. In the next step, a simplified explanation of how vulnerability management currently works at GOSP is shown focusing on the one hand on the back end, namely the data preparation process with its different steps, and on the other hand on the front end, showing how the vulnerabilities are currently analyzed, reported, and shared to the CISOs. Further, this paper will propose a solution to the problems that emerged describing the technical approach used, and finally, an interpretation of the results is discussed focusing on both the improvements made and the issues that still need to be solved to reach an optimal, completely automized, and transversal tool.

2. The Cost Impact of Security Vulnerabilities

In the modern world, cyberculture has emerged as a common and unavoidable source of information exchange. At the same time, cybercriminal activities have increased rampantly because of the exponential growth in the use of cyberspace. The primary cause of this growth is the daily and transversal overuse of Web applications which contain design flaws, also known as vulnerabilities, that cybercriminals exploit through a cyber-attack to obtain unauthorized access to the systems. On this matter, cybersecurity focuses on preserving the integrity, confidentiality, and timely availability of systems, information, or data and its main goal is to secure information by detecting, preventing, and responding to cyber-attacks.

It is however fundamental to clarify that only when a threat coincides with a corresponding vulnerability does a risk exist, and once this risk exists, it can lead to potential corruption of the system with severe consequences for the company or individual affected. Therefore, preserving the security of IT systems automatically implies the necessity of a good vulnerability management process.

The first step that was carried out to analyze GOSP's vulnerability management was to detect the possible consequences that poor vulnerability management brings to then identify the flaws concretely affecting the efficiency of the process in the company.

To fully understand the threat that vulnerabilities represent, it is important to analyze, quantitatively when possible or qualitatively, the cost factors associated with a breach deriving from vulnerabilities. To do so, the research carried out in the book "The True Cost of Information Security Breaches and Cyber Crime" by Michael Krausz and Professor John Walker, two specialists in the information security field, was used.

The main costs associated with cyber risks deriving from security vulnerabilities comprise both financial costs, which can be averagely estimated, and reputational costs, which can only be guesstimated.

Financial costs include both direct and indirect costs. On the one hand, direct financial costs represent those costs that, consequently to a security breach, the organization must cover. More specifically, these costs include work time, overtime, external cost, equipment leases, legal costs, and all the other costs that can be directly attached to the occurrence of the breach itself. Based on the specialists' extensive experience with corporate cases, it can be assumed that direct financial costs usually range between £10,000 and £100,000 for an easy-to-remedy breach, going up to £500,000 for a more complex breach, and reaching over £500,000 for targeted attacks. On the other hand, indirect financial costs include the costs of lost productivity deriving from a cyber-attack, and all the other costs that not directly but causally relate to the breach. Unlike direct financial costs, these costs are hard to estimate as they are associated with the procedures connecting to the business process that was violated and evolve differently based on the number of processes and entities involved.

When talking about reputational costs, considering GOSP as the organization at interest, we refer to customer reputational costs which incur due to a loss of credibility and trust within the customers resulting in a direct impact on the bottom line.

Considering all these factors, we can estimate that vulnerabilities have, if exploit by a corresponding threat, a significantly high impact on any business and must therefore be kept under strict control and must be remediated in the shortest time possible.

3. GOSP

Generali Operations Service Platform (GOSP) is a joint venture between Generali Group and Accenture that aims at accelerating the digitization of Generali Group's business processes and the adoption of a cloud-centric model with the foremost objective of creating a package of cyber insurance services that help corporate and SMEs (small and medium-sized enterprises) clients quickly and effectively recognize, respond to, and recover from cybersecurity threats.

As previously discussed in section 2, the consequences that incur when a cyber threat exploits a corresponding vulnerability are severe. On these terms, one of GOSP's future objectives is to ward off or, in extreme cases, solve as fast as possible any vulnerability that can lead to a corresponding cyber threat by moving the process of vulnerability management towards a more automatic approach through data visualization.

4. Vulnerabilities Classification at GOSP

A structured, correct, and most of all automatized process to manage the vulnerabilities that affect any organization's IT systems is fundamental to optimizing the available resources,

maximizing the revenues, and minimizing the time loss, as a manual approach would result in a time- and resource- intensive procedure.

The metrics and procedures behind vulnerability management are complex and therefore need a careful and detailed explanation. In the following paragraph, some clarifications and technical aspects will be discussed to guide the reader through the topics covered in the paper, more specifically by explaining the variables considered to classify the vulnerabilities and by explaining how the current process of vulnerability management works at GOSP.

To have an efficient vulnerability management process and clear analyses, vulnerabilities must be classified. The main variables used to classify vulnerabilities at GOSP are the perimeter, the severity, the status, the asset owner responsible for the vulnerability, and the typology.

The perimeter can either be internal or external based on the IP address of the device subject to the vulnerability itself: if the IP address identifying the device on the network is internal, the vulnerability will be classified as internal and, on the other hand, if the IP address is external, the vulnerability will be classified as such.

The number of vulnerabilities discovered and reported during the recent decades is enormous and not all the vulnerabilities have the same impact on the organization's IT systems. Therefore, information technology management faces a significant challenge in better classifying and prioritizing vulnerabilities based on their severity. Although several methodologies for ranking and scoring vulnerabilities have been proposed, one of the most common methods used to classify a vulnerability is by supplying a qualitative measure of its

severity using the universal Common Vulnerability Scoring System (CVSS v3.0[1]).

The CVSS score is calculated through three metric groups: base, temporal, and environmental[2]. Based on the score assigned, which ranges from 0 to 10, the severity of the vulnerability can either be classified as none, low, medium, high, or critical as shown in *Table 1*.

Severity	Score
None	0
Low	0.1 – 3.9
Medium	4.0 – 6.9
High	7.0 – 8.9
Critical	9.0 – 10

Table 1

Each vulnerability, once identified, follows a specific workflow with different ordered stages, namely: under analysis, pending, open, notified, ready for escalation, risk opened, remediated by owner, and finally closed[3]. Each of these stages represents the status of the vulnerability at the time of the considered extraction.

In GOSP's process of vulnerability management, the Vulnerability Management and Prevention team notifies each vulnerability to a specific department which is then responsible to remediate and close the vulnerability. Departments, and consequently the corresponding vulnerabilities, can be associated with three main asset owners, namely GOSP, Local, and Under Evaluation[4].

Vulnerabilities can be mapped to different types based on which is the cause of the vulnerability itself. The main typologies used by GOSP to classify the vulnerabilities are obsolete systems,

[1] In GOSP's vulnerability management process, to classify a vulnerability based on the severity, if the CVSS v3.0 score is not available, the classification will be made based on the CVSS v2.0 score
[2] The Base metrics produce a score ranging from 0 to 10, which can then be modified by scoring the Temporal and Environmental metrics
[3] Further explanations of the specific stages are given in Appendix B
[4] Further explanations of the specific asset owners are given in Appendix B

security misconfiguration, insecure deserialization, remote code execution, DoS (denial of service), and other[5].

5. Problem Formulation

To propose a solution that can improve vulnerability management at GOSP, it is necessary to point out which are the main problems affecting its efficiency. To do so, the current vulnerability management process must be analyzed.

5.1. Vulnerability Management at GOSP

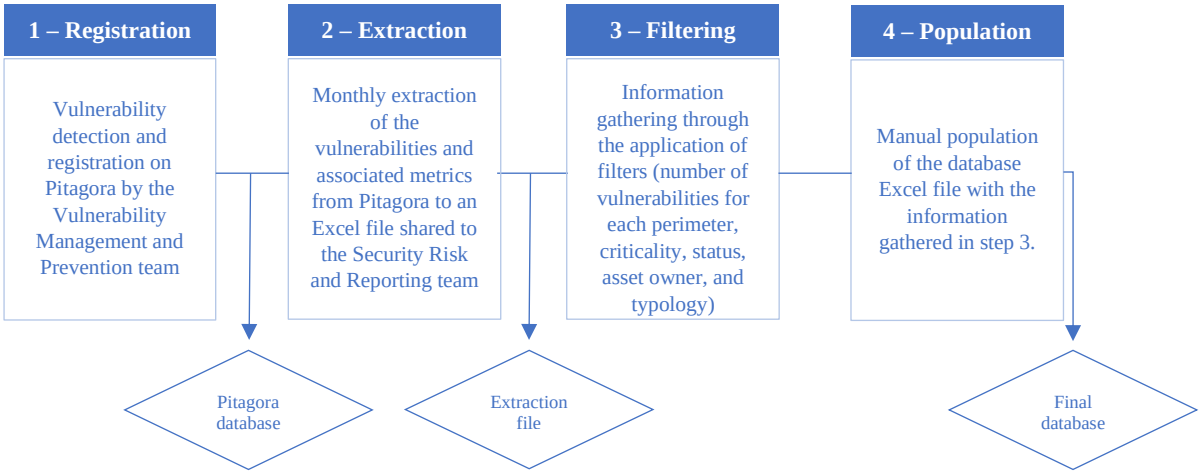


Figure 1 – Current data curation at GOSP

The process that goes from the detection of the vulnerabilities to the insertion of the information needed into the final database is shown in Figure 01.

Once the final database is populated, the Security Risk and Reporting team shares the data with the CISOs of the legal entities of interest and GOSP's CSO through a PowerPoint monthly report considering the data of the last three extractions. The report displays through various

[5] Further explanations of the specific typologies are given in Appendix B

graphs the number of vulnerabilities classified on the one hand by status for each perimeter, severity, and asset owner, and on the other hand by typology for each perimeter. An extract of the currently used final database and an example of a vulnerability monthly report can be seen in Appendix C.

5.2. Problem

Accurate and timely data is a fundamental element of management, decision-making, and productivity. Especially for a process like vulnerability management in which a slow handling procedure leads to a higher chance of receiving cyber-attacks, the steps and analyses must be fast and accurate.

By analyzing GOSP's vulnerability management process, the first and most impacting problem that arises is that the whole process is performed with an extremely manual approach.

Moreover, GOSP's current reporting focuses only on displaying the number of vulnerabilities for each classification by integrating just a portion of the metrics available and therefore losing a significant number of relevant analyses, resulting in a report which is informative yet not relevant from a decision-making point of view.

In conclusion, the two main problems identified and for which a solution is proposed are the manual approach used in the process and the lack of relevant analyses needed to guide the decision-making.

5.3. Solution

Foremost, the solution aims to provide a data-driven answer to the problems raised: the main goal is to present a tool that can help the organization save time and resources and at the same time improve the quality of the analyses performed. More specifically, the approach proposed

has two major objectives: to speed up the data preparation processes through automation, and secondly, to retrieve relevant insights from the data through a Power BI dashboard enabling a focus on the most critical aspects affecting the efficiency of the vulnerability management process to help the decision-making in correctly allocating investments in terms of security awareness, resources, or workforce in those departments and asset owners that represent the bottlenecks.

6. Data Curation

The decisions that business leaders make are only as good as the data that supports them. As mentioned in the previous paragraphs, the database that GOSP currently uses to analyze and consequently report vulnerabilities is poor in terms of possible insights that can be extracted from it. Therefore, the first aspect to improve is to implement an automated transformation of data into relevant and clean forms which can be used for high-profit purposes.

As shown in Figure 2, data curation in the new vulnerability management process consists of three main phases namely, data collection, data cleaning, and data aggregation.

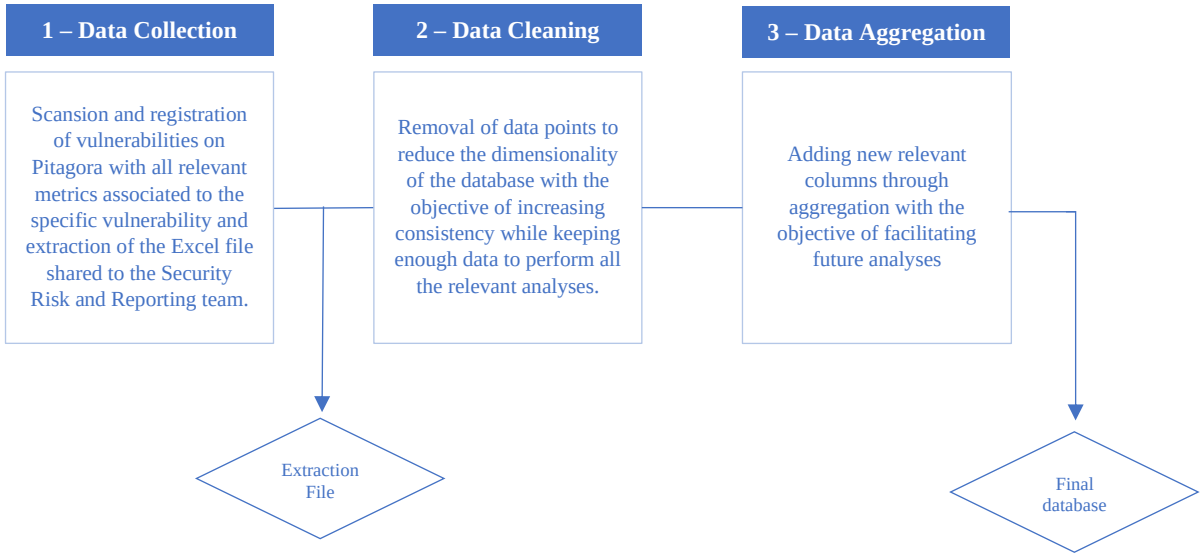


Figure 2 – Data curation in the new vulnerability management process

6.1. Data Collection

The scanned vulnerabilities are automatically registered on the Pitagora software together with all the metrics related to the specific vulnerability.

With the purpose of building a security dashboard that aims at guiding the CISOs and CSO through a critical overview of the vulnerabilities affecting the company and its clients, the Security Risk and Reporting team requested the Vulnerability Management and Prevention team a monthly extraction from Pitagora containing the metrics considered useful to perform both the existing and new analyses. More specifically, the features received from the requested extraction and their characteristics are displayed in Table 2. Please note that data in terms of number of values and missing values refer to the extraction made in October 2022.

Column Name	Type	Description	Example[6]	Number of Values[7]	Missing Values[8]
ID	Categorical	Vulnerability ID	2096593	39453	0%
Internal IP	Categorical	IP address. If the IP for the specific vulnerability is not internal, this field will be blank	10.232.1.29	-	-
External IP	Categorical	IP address. If the IP for the specific vulnerability is not external, this field will be blank	193.57.145.110	-	-
Application Name	Categorical	Name of the application connected to the IP address	AML common solution	464	98.8%

[6] If in this field the value "-" is displayed, it means that the data is confidential, and an example cannot be displayed.
[7] If in this field the value "-" is displayed, it means that this calculation is not applicable to the specified variable. For example, for the Internal IP and External IP metrics, displaying the number of values would be misleading as each vulnerability can either have the Internal IP or the External IP field filled.
[8] If in this field the value "-" is displayed, it means that this calculation is not applicable to the specified variable. For example, for the Internal IP and External IP metrics, displaying the number of missing values would be misleading as each vulnerability can either have the Internal IP or the External IP field filled. The percentage of missing values is calculated based on the expected number of values for each variable, for example, a notify date is not expected for each vulnerability but for the ones which are at a stage in the workflow after and included the notification stage.

Title	Categorical	Title of the vulnerability	SSL Version 2 and 3 Protocol Detection	39453	0%
CVSSv2	Numerical	Severity score assigned to the vulnerability based on the CVSS version 2 method	9.2	39255	0.5%
CVSSv3	Numerical	Severity score assigned to the vulnerability based on the CVSS version 3 method	9.0	36.584	7.3%
Status	Categorical	Stage of the vulnerabilities' workflow at the time of the extraction	Open	39453	0%
Country	Categorical	Country where the vulnerability was detected	Italy	39452	0.002%
Asset Legal Entity	Categorical	Legal entity where the vulnerability was detected	-	39453	0%
Department Name	Categorical	Department to which the vulnerability has been assigned to be remediated	-	33165	15.9%
First scan date	Date-time	Date and time in which the vulnerability is first registered in Pitagora	2021-05-12T 02:00	39436	0.04%
Notify date	Date-time	Date and time in which the vulnerability is assigned to its asset owner	2021-06-14T00:03	34059	13.7%
Acceptance date	Date-time	Date and time in which the vulnerability is accepted by the asset owner to which it's assigned	2021-06-30T14:45	551	98.6%
Due date	Date-time	Date and time in which the vulnerability is due	2022-01-11T10:00	33130	16%
Remediation date	Date-time	Date and time in which the vulnerability is remediated by its asset owner	2021-12-13T17:25	692	98.2%
Closing date	Date-time	Date and time in which the vulnerability is closed	2021-12-14T09:12	22289	43.5%
rsaArcherRiskId	Categorical	Risk Associated to the vulnerability. The risks are registered in Archer.	2001283_IT097	4133	89.5%

Table 2 – features requested in the extraction file

6.2. Data Cleaning

Data cleaning is a method of managing the data accumulated by businesses and organizations by fixing or removing irrelevant, incorrect, corrupted, incorrectly formatted, duplicate, or incomplete data within a dataset. Although the raw data collected provides a valuable resource to companies, allowing them to critically examine their efforts to find flaws and inefficiencies, it often requires careful management.

There are two main steps involved in the data cleaning process that aim at removing unnecessary data points that for now only impact the efficiency of the process slowing it down.

As explained in section 4, two common uses of the universal CVSS score are calculating the severity of vulnerabilities discovered on one's systems and as a factor in prioritization of vulnerability remediation activities: the highest the score, the highest the prioritization that must be given to the corresponding vulnerability. Pitagora collects all the vulnerabilities regardless of the severity with the result of having a database containing multiple information on thousands of vulnerabilities. It can be easily understood that deciding to include all the vulnerabilities in the analyses would drastically reduce the efficiency and promptness of a process which, by definition, must be extremely rapid and efficient as any added time can result in critical consequences for the entire business. Based on these considerations, GOSP's CSO decided that an optimal trade-off between maximum productivity and maximum amount of relevant data treated was to consider only those vulnerabilities with a CVSS score higher than 7, namely all the vulnerabilities classified as either high or critical.

To further maximize the efficiency, the vulnerabilities with none, low, and medium severity are directly excluded in Pitagora before the extraction is made: before proceeding with the extraction of data from Pitagora, the responsible member of the Vulnerability Management and

Prevention team will filter the vulnerabilities selecting the severity as high or critical. This results in having a smaller excel extraction file on which any further calculation can be computed faster.

In the last years, the vulnerability management process at GOSP evolved significantly simultaneously with an increase in security awareness: in the first years, vulnerability management represented just a small focus for the company as its possible repercussions on the organization were underestimated. After recognizing the sources and understanding the destructive risks that can derive from cyber-attacks, in October 2021 GOSP decided to invest in a new performing massive process of vulnerability management.

Given this scenario, GOSP's CSO decided to exclude from any analyses, and therefore from the extraction file, all those vulnerabilities with a closing date prior to October 2021 with the objective of having a more consistent yet relevant database.

6.3.Data Aggregation

Starting from the existing analyses made on the monthly reports and keeping in mind the main goal of providing the CISOs and CSO with a tool that could help the decision-making, the Security Risk and Reporting team at GOSP decided to add new features to the database through the aggregation of already existing features to ease and speed up the analyses performed.

The features added can be classified into two categories, namely categorical and temporal features. Categorical features aim at mapping more efficiently the vulnerabilities to the categories discussed in section 4, while temporal features are used as KPIs in measuring efficiency. A detailed explanation of the added features is shown in table 3.

Column Name	Type	Description	Example	Number of Values	Missing Values
Perimeter	Categorical	Either internal or external based on the information contained in the column "Internal IP" and "External IP"	Internal	38019	0%
Severity	Categorical	Either high or critical	Critical	38019	0%
Asset Owner	Categorical	Either GOSP, Local, or Under Evaluation based on the department to which the considered vulnerability is assigned.	GOSP	38019	0%
Typology	Categorical	Typology assigned to the vulnerability based on its title: a merge between the extraction file and an existing file containing a typology for each possible vulnerability title.	Obsolete System	38019	0%[9]
Notification Time	Temporal	Number of days to assign vulnerability, calculated as the difference between the notify date and first scan date	34	33714	12.9%
Closing Time	Temporal	Number of days to close vulnerabilities, calculated as the difference between the closing date and the notify date	12	16901	47.16%

Table 3 – added features

7. Dashboard

Once the data was collected in a clean, consistent, and complete database, the focus moved to the second issue affecting GOSP's vulnerability management process: the quality of the analyses performed. To mitigate this problem, a security dashboard was built. The two main

[9] This value must always be 0%: a vulnerability always has a title, and this title is assigned to a typology. If a vulnerability with a new title is scanned, this title must be manually mapped to a typology in the typology sheet used in the merge. The percentage of missing values is calculated based on the expected number of values for each variable, for example a notify date is not expected for each vulnerability but for the ones which are at a stage in the workflow after and included the notification stage.

goals of the dashboard are to inform about the categorical distribution of the vulnerabilities and analyze the efficiency of each department in dealing with vulnerabilities to help the decision-making. At the beginning of the dashboard, there is a summary[10] containing both perspectives, and then for each of the two goals, a detailed portion of the dashboard is dedicated.

More specifically, the dashboard is composed of three sheets: "vulnerabilities", "notification efficiency", and "closure efficiency". Each of the three sheets is divided in three main sections: the user can apply any of the filters shown in section 1 that will determine the view of the data displayed in section 2 and the graphs reported in section 3. Furthermore, the filters applicable to the notification efficiency sheet are the same as the ones in the overview sheet and will be adapted synchronously, on the other hand, in the closure efficiency sheet the only filter that will not sync with the previous sheets is the temporal one as it considers as input the notification date instead of the first scan date.

The dashboard can be analyzed from two different points of view namely GOSP's CSO, who has access to a general overview of the clients and can see analyses for each legal entity, and the CISOs who only have details, both in terms of vulnerabilities' classification and efficiency, about their legal entity. More specifically, the dashboard shared with each CISO will have a filter applied to consider the legal entity for which they are responsible.

The purpose of this section is to guide the reader through the main steps taken to reach the goals proposed, therefore, to avoid redundant representations, the figures displayed in the following sections will be based only on GOSP's CSO point of view as the dashboard shared

[10] The summary sheet can be seen in Appendix D

to the CISOs is just a narrower view obtained through the application of a filter on the legal entity field. Considerations will however be made based on both points of view to show the reader a possible approach used to interpret the data represented.

Please note that to build the dashboard, internal and confidential data was used. Therefore, the examples displayed further in this paper will have some data that was anonymized[11], and some that were obscured[12].

7.1.Vulnerabilities classification

The classification by status aims at helping the user in identifying how effectively vulnerabilities are being managed in terms of resolution: an indicator that vulnerability management is working effectively can be evaluated by looking at the distribution of vulnerabilities through the different stages of the workflow.

[11] Each name of the country was changed to Country x, where x represents a different number for each country considered

[12] This data could not be changed as it would have affected the data curation process: the column of the asset owner is built based on the department name

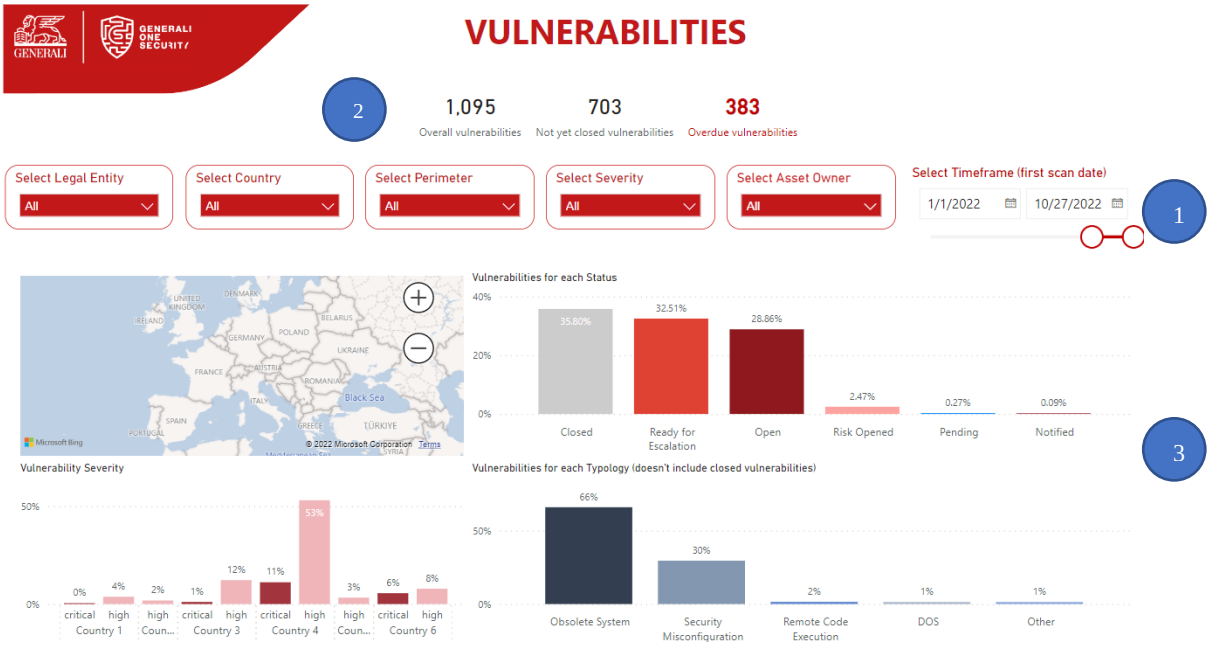


Figure 3 – Dashboard section on vulnerabilities' classification

Figure 3 represents an example of the view the user obtains in the overview sheet when filtering the vulnerabilities considering only the ones scanned in 2022. The two graphs displayed on the right are informative and aim at representing the distribution of vulnerabilities based on the two main classifications GOSP uses which are the status and the typology.

As can be seen from the displayed example, although closed vulnerabilities represent the highest value, the percentage of open vulnerabilities is almost 30%. Therefore, we can assume that there is a lack of efficiency either in the Vulnerability Management and Prevention team in assigning the vulnerabilities or in the departments in accepting the assigned vulnerabilities. This formulated assumption can be further analyzed using the sheet dedicated to the notification efficiency which will be discussed in section 7.2..

On the other hand, the classification by typology aims at helping understand the causes of the vulnerabilities with the final goal of guiding the CSO in deciding how to distribute a potential investment. In the examined scenario, almost 70% of the vulnerabilities scanned in 2022 have as typology Obsolete System meaning that the technology used is not up to date. Having

obsolete systems compounds existing vulnerabilities as the product will no longer receive security updates and the latest security mitigations are not present. These two factors allow attackers to identify vulnerabilities more easily and increase the impact of vulnerabilities making exploitation more likely to succeed. Therefore, a solution to overcome these problems is to invest in updating or, in extreme cases, changing the technology used.

Finally, the graph on the bottom-left corner represents the distribution of vulnerabilities by severity showing for each country the percentage of high and critical vulnerabilities. It can be seen from the graph displayed in Figure 3 that almost all the countries have a significantly higher number of high vulnerabilities compared to the critical ones. Nevertheless, in Country 6, whose vulnerabilities represent 14% of the overall vulnerabilities scanned in 2022, the percentage of critical vulnerabilities (6%) is almost as big as the percentage of high vulnerabilities (8%) meaning that an intervention must be carried out in this country. To better understand which are the aspects that led to this significant number of vulnerabilities with critical severity, the user can filter the views based on the country that is to be considered. The example of the view displayed filtering for Country 6 is shown in Appendix D. Of the vulnerabilities registered in this country, almost 80% are due to obsolete systems, therefore, merging this information with the one formulated when analyzing the distribution for typology, investing in changing or updating out-of-date systems and software might bring to a better scenario also for Country 6 with fewer vulnerabilities and lower severity.

7.2.Vulnerability management efficiency

The second portion of the dashboard aims at measuring through different KPIs the efficiency of vulnerability management within GOSP and its clients. The two main aspects affecting the

efficiency of the vulnerability management are the notification (Figure 5) and closure (Figure 6) processes, one dedicated sheet for each of the two processes was built.

Once the Vulnerability Management and Prevention team assigns the vulnerability to its asset owner, the latter can accept or decline the assigned vulnerability and if the vulnerability is declined a new notification must be made. As soon as the first assignment is made, a notification date is registered under the field “notify date”. However, anytime a vulnerability is refused by the asset owner and a new notification process starts, the notification date of the new assignment will be overwritten on the existing one. Therefore, a low efficiency in the notification process can be caused either by a low efficiency of the Vulnerability Management and Prevention team in assigning the vulnerabilities to their asset owner, or a low efficiency of the asset owners in accepting or declining the assigned vulnerability.

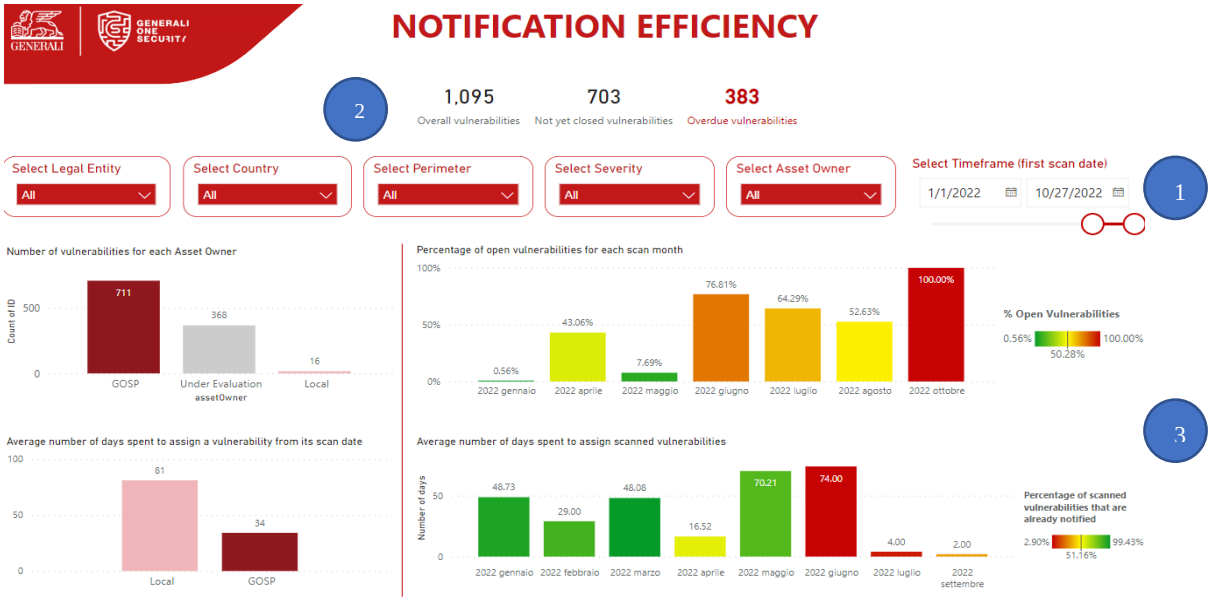


Figure 4 – Dashboard section on notification efficiency

To quantify the notification efficiency two methods were used: one considering the number of vulnerabilities that have not been assigned yet, and the other considering the time spent to complete this process.

The two graphs displayed at the top of the sheet shown in Figure 5 use the number of assigned vulnerabilities as a measure of efficiency: the first graph, displayed on the left side, considers the number of vulnerabilities assigned to each asset owner, while the second one, displayed on the right side, considers the percentage of not yet assigned vulnerabilities for each scan month to highlight which are the least productive months in terms of notification of vulnerabilities. On top of displaying the number of vulnerabilities notified to each asset owner, the first graph can be used to perform a further efficiency analysis. As previously explained, analyzing the number of vulnerabilities for which an owner has not been decided yet helps to guesstimate the efficiency of the Vulnerability Management and Prevention team in notifying for the first time a vulnerability to its asset owner. In the example displayed in Figure 5, of the overall 1'095 vulnerabilities scanned in 2022, 368 have the asset owner classified as Under Evaluation meaning that, as of now, the Vulnerability Management and Prevention team has never assigned one-third of the vulnerabilities to their asset owner.

On the other hand, when considering the notification time which is represented in the two graphs at the bottom of the visual, the performance of the Vulnerability Management and Prevention team and the one of the asset owners cannot be split because of the previously explained complex structure of the notification process. Therefore, the notification time is used as an aggregated measure to estimate the performance of both the Vulnerability Management and Prevention team and the asset owners.

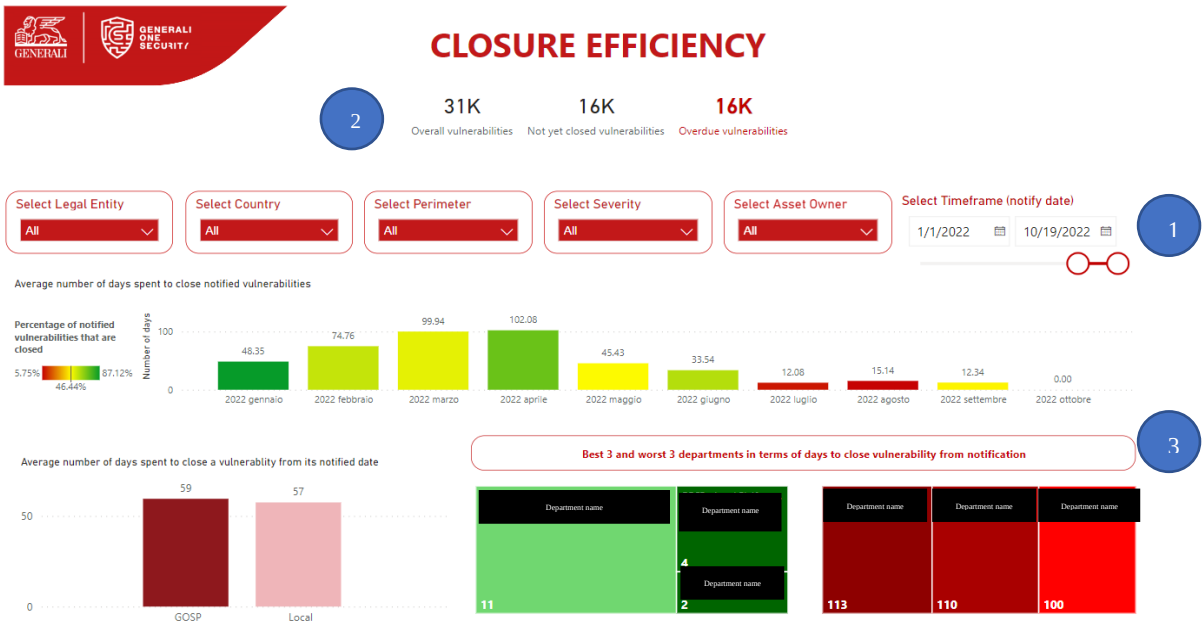


Figure 5 - Dashboard section on closure efficiency

Once a vulnerability is accepted by the department to which it was assigned, it is the department's responsibility to close it. The sheet shown in Figure 6 aims to give an estimation of the how efficiently the vulnerabilities are being closed from the moment of notification.

The first graph shows the average number of days needed to close the vulnerabilities from the moment of notification to the decided department, highlighting the percentage of notified vulnerabilities that have been successfully remediated for each notification month; the aim is to highlight the most critical months in terms of closure.

The lower part of the sheet focuses on the people responsible for the closure of vulnerabilities. The idea is to identify the departments and asset owners that are affecting the efficiency of vulnerability management using as a metric the average number of days that it took to close a vulnerability from the moment of its notification. This information aims at helping the CSO to make targeted investments in terms of resources and security awareness on the bottlenecks of the process with the goal of improving its efficiency by reducing the time spent to close vulnerabilities and consequently reducing the risk of a cyber-attack.

8. Results

GOSP's Security Risk and Reporting team is currently styling each month ten vulnerability reports, one to the CISO of each of the nine legal entities, and one to GOSP's CSO. For each report the respective portion of the database must be manually updated, as explained in section 5.1., and the manual selection of data from Excel must be done in Power Point. This same operation is repeated every month with the result of a great time-investment. Furthermore, each of the top manager, after examining the reports, must perform additional and separate analyses to inspect the critical aspects emerged and consequently implement targeted actions.

Including an automatized data curation process in the database population process and building a dashboard which focuses on displaying relevant analyses, results in a huge time saving for the company: in the new process, anytime a new monthly extraction is made, the new data must be overwritten on the existing database file according to its structure and a refresh of the data must be performed on Power BI.

The tables displayed below show a time-comparison between the old (table 4) and the new (table 5) vulnerability management processes with the different actions that must be performed to style the monthly reports. Furthermore, although it cannot be quantified, there will be an additional time saving factor for the entities receiving the monthly reports in terms of interpretation of the results as an instrument for decision-making given the different nature of the analyses displayed in the old reports and in the dashboard.

Old vulnerability management process		
Action	Time needed for one report[13]	Total time needed[14]
Database population[15]	8 minutes	80 minutes
Reporting	4 minutes	40 minutes

Table 4

New vulnerability management process	
Action	Total time needed[16]
Database population	3 minutes
Reporting	10 seconds

Table 5

9. Limitations and future work

Although the process improved drastically with the introduction of automation tools, given that the massive process of vulnerability management was only introduced in GOSP in October 2021, there is still room for improvement. The next main steps that must be taken are making the data more consistent reducing the missing values, starting from those which alter the reality of the analyses performed, as for example temporal data; an additional investment in scansion tools must be made to have complete information about vulnerabilities allowing more realistic and thorough analyses. At a further stage, the dashboard will serve as tool to have real-time analyses on vulnerabilities making the extractions automatic and increasing their frequency.

10. Conclusion

GOSP treats large amounts of security confidential data to guide several clients among Generali Group in increasing the security affecting their systems, information, and data. Accordingly, bad vulnerability management, which leads to poor cyber security, translates into a bad service offered by GOSP. As previously discussed, poor service consequently leads to significant

[13] The time reported is an estimation based on the experience made
[14] Calculated as the time needed for one report times the number of reports (10)
[15] Includes all the steps from the extraction of the File from Pitagora until the population of the final database
[16] The new database is not divided by legal entity unlike the old one, therefore, only the total time is reported

indirect financial costs deriving from complaints filed by the clients because the company itself failed to meet its service level commitments. Moreover, especially for organizations treating confidential data, a breach would translate into huge repercussions for the entire business as it would impact the availability, integrity, and confidentiality of the data treated consequently ruining the reputation of the company among the clients.

The new tools introduced, represent a strong starting point to help the company's top manager drastically reduce these risks by moving vulnerability management towards a more efficient and data driven approach.

REFERENCES

BISCONTINI, TYLER. “Data Cleaning”. *Salem Press Encyclopedia of Science*, 2020

HUMAYUN, M., NIAZI, M., JHANJHI, N. “Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study”. Arabian Journal for Science and Engineering, 2020. https://doi.org/10.1007/s13369-019-04319-2

ISO/IEC. *Information Technology - Security Techniques - Vulnerability Disclosure*. https://www.iso.org/obp/ui/#iso:std:iso-iec:29147:ed-2:v1:en. ISO/IEC 29147, 2018

JOINT TASK FORCE TRANSFORMATION INITIATIVE. *Guide for Conducting Risk Assessments*. NIST, 2012.

KRAUSZ, M., and WALKER, J. *The True Cost of Information Security Breaches and Cyber Crime*. IT Governance Publishing, 2013. http://www.jstor.org/stable/j.ctt5hh6x8.

NATIONAL CYBER SECURITY CENTRE. “Obsolete Products”. *Security Guidance*, 2021. https://www.ncsc.gov.uk/collection/device-security-guidance/managing-deployed-devices/obsolete-products

SPANOS, GEORGIOS, AND LEFTERIS ANGELIS. “Impact metrics of security vulnerabilities: analysis and weighing”. *Information Security Journal: A Global Perspective*, 2015.

VON SOLMS, B., VON SOLMS, R. “Cybersecurity and information security—what goes where?” Information and Computer Security, 2018.

APPENDIX

A. Cyber security terminologies

Term	Definition
Cyberspace	Global domain within the information world whose distinct characteristics is the use of the electronic and electromagnetic spectrum to create, update, store, share, and exploit information with the help of interconnected and dependent networks using the latest information and communication technologies
Vulnerabilities	Flaws in a system or its design that allow an attacker to execute malicious commands, access data in an unauthorized way, and/or conduct various denial-of-service attacks
Threats	Actions taken to gain benefit from security breaches in a system and negatively impact it
Risk	Loss of confidentiality, integrity, or availability of information, data, or information (or control) systems
Attacks	Actions taken to damage a system or disturb its routine operations by exploiting vulnerabilities using various tools and techniques. Attackers launch these attacks to achieve their malicious goals, either for self-satisfaction or for financial reward

IPS (intrusion prevention system)	Network security tool that continuously monitors a network of malicious activity and takes action to prevent it, blocking, or dropping it when it occurs,
WAF (web application firewall)	Helps protect web applications by filtering and monitoring HTTP traffic between a web application and the internet.
Phishing	Fraudulent action of sending emails purporting to be from reputable companies to induce individuals to reveal personal information.
Malware	Software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system
Antimalware	Type of software program created to protect IT systems and individual computers from malicious software, or malware
Spam	Irrelevant or unsolicited messages sent over the internet, typically to a large number of users, for the purposes of advertising, phishing, or spreading malware
Antispam	Services and solutions that focus on blocking and mitigating the effects of spam on the users targeted
CSO	Chief Security Officer: is the executive leader responsible for the security of the physical and digital assets of the business
CISO	Chief Information Security Officer: is the executive leader responsible for the security of digital information assets

B. Classification

a. Vulnerability status: workflow stages

Status	Description
Open	Vulnerabilities enter Pitagora in the Open state
Under Analysis	Used when it is not possible to identify/assign the vulnerability to a specific owner who could be able to manage it. To be considered as an exception to the process. Only settable by a Vulnerability Manager
Notified	The vulnerability is assigned to its asset owner
Pending	Vulnerabilities have been accepted and are being processed. The remediation due date, as well as the remediation start date, have been set
Remediated by Owner	The vulnerabilities have been remediated; the closing date has been specified
Mitigated	This status is set manually when remediation cannot be put in place and a workaround has been found. For instance, it can be set in special cases such as extending the support of an OS
Ready for Escalation	The vulnerability has exceeded the process card time (in any way). For each vulnerability not fixed within the time frame provided by the process card for that type of vulnerability.
Risk Opened	The Technical Feed was escalated to Archer and the RiskID was assigned

Closed	The vulnerability is closed meaning it has been solved by its asset owner

b. Vulnerability asset owners

Asset Owner	Description
GOSP	All the vulnerabilities assigned to GOSP teams
Local	All the vulnerabilities directly assigned to Customer Local teams
Under Evaluation	All the vulnerabilities for which Asset Owner evaluation is still ongoing

c. Vulnerability typologies

Typology	Description
Obsolete System	The software is not up to date, making it easier for attackers to exploit the vulnerability and perform an attack
Security Misconfiguration	Essential security settings are either not implemented or implemented with errors giving attackers unauthorized access to system data and functionality
Insecure Deserialization	User-controllable data is deserialized* by the server
Remote Code Execution	Remote attackers exploit a remote third-party library containing a vulnerability that is connected to the local machine which may not directly contain vulnerabilities

DoS (denial of service)	The attacker exploits this vulnerability to throw a denial-of-service attack which focuses on making a resource (site, application, server) inaccessible to its intended users for the purpose it was designed
Other	The vulnerability cannot be mapped in any of the above-cited typologies

* Serialization is the process of converting complex data structures into a "flatter" format that can be sent and received as a sequential stream of bytes, while deserialization is the process of restoring this byte stream to a fully functional replica of the original object, in the exact state as when it was serialized.

C. Vulnerabilities monthly report

The following figures represent an extract of the final database used and the graphs shared in the vulnerabilities monthly report for one of the legal entities considered.

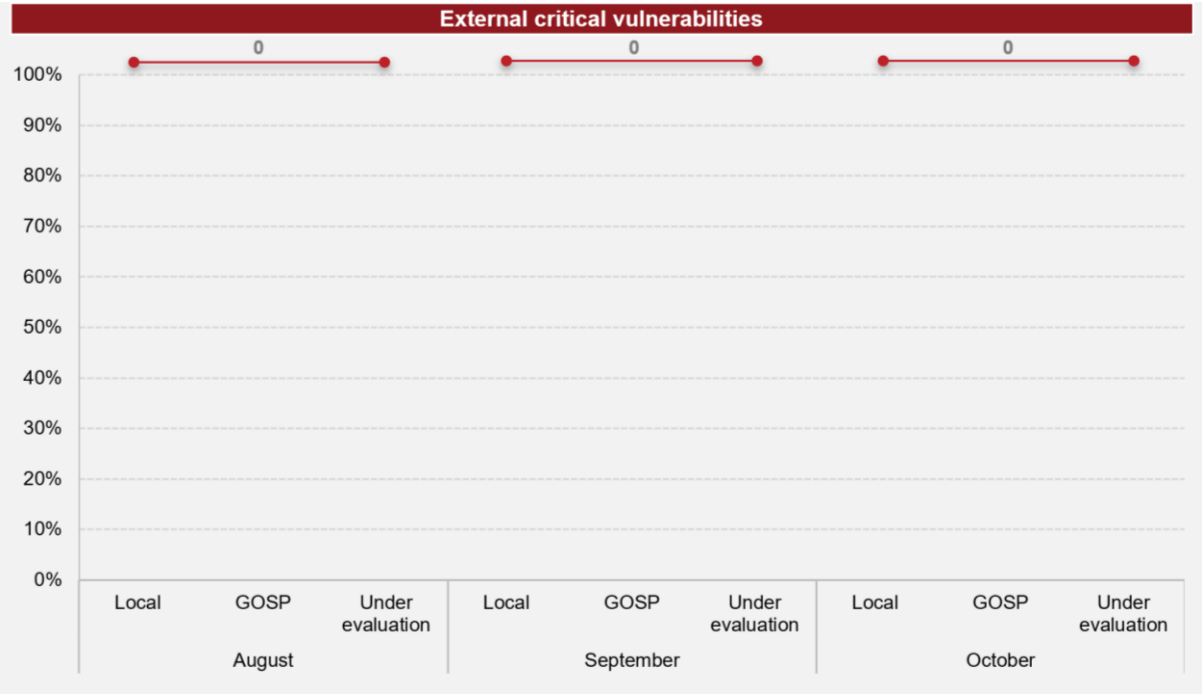
a. Current Database

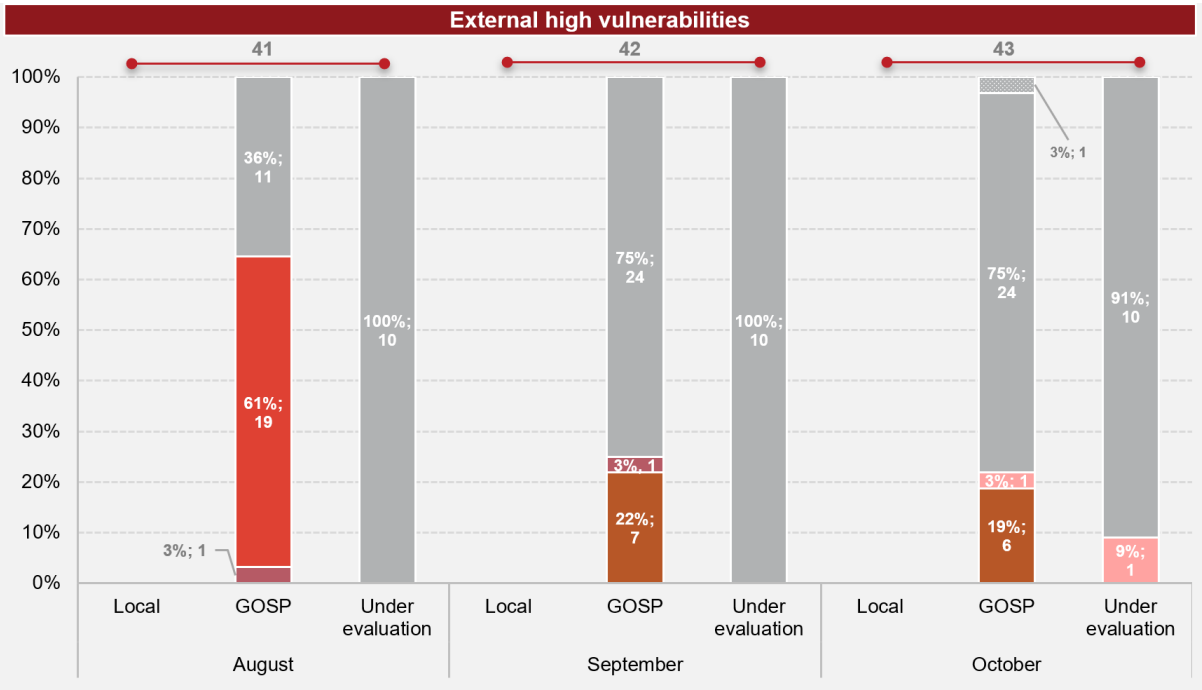
Portion of the database used to compile the PowerPoint reports representing external critical vulnerabilities for the legal entity considered.

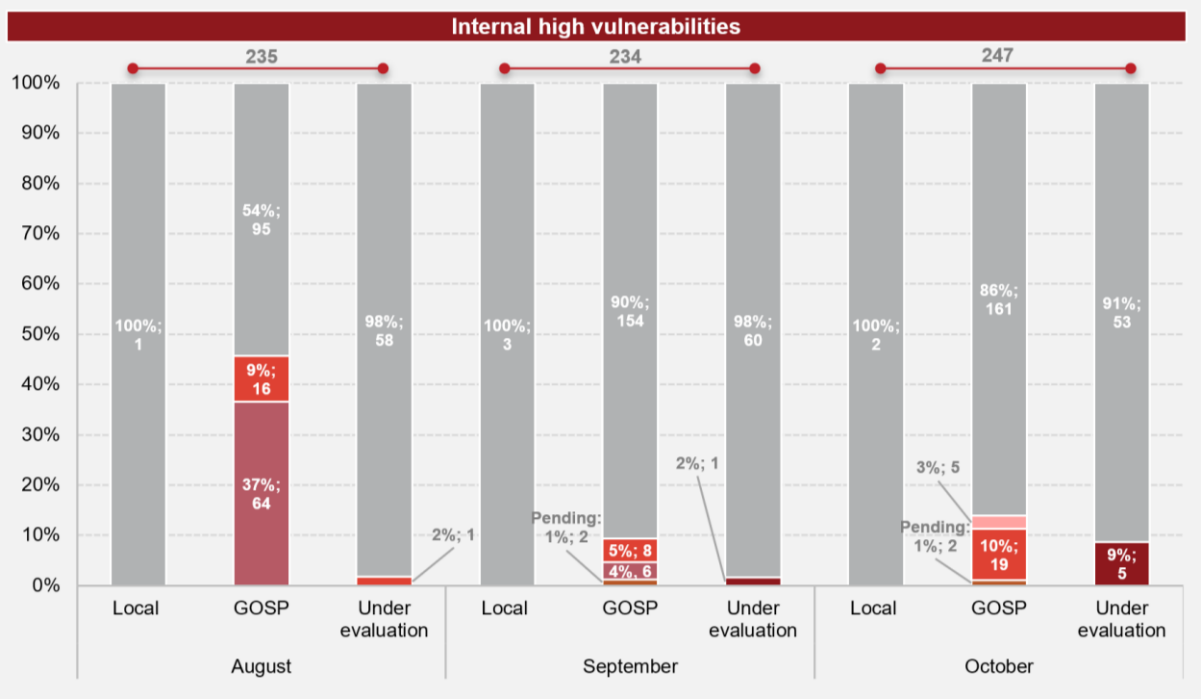
		# Under analysis	# Under analysis current month	# Pending	# Pending current month	# Open	# Open current month	# Notified	# Notified current month	# Ready for escalation	# Ready for escalation current month	# Risk opened	# Risk opened current month	# Remediated by owner	# Remediated by owner current month	# Closed	# Closed current month
March	Local									3							
	GOSP									8						1	
	Under evaluation					1				31							
April	Local																
	GOSP							2		40						1	
	Under evaluation					1											
May	Local							8									
	GOSP							9		11						3	
	Under evaluation					1										9	
June	Local									8							
	GOSP							2		19						3	
	Under evaluation															9	
July	Local																
	GOSP							10		17						5	
	Under evaluation															9	
August	Local																
	GOSP							1		19						11	
	Under evaluation															10	
September	Local																
	GOSP			7				1								24	
	Under evaluation															10	
October	Local																
	GOSP			6								1				25	
	Under evaluation											1				10	

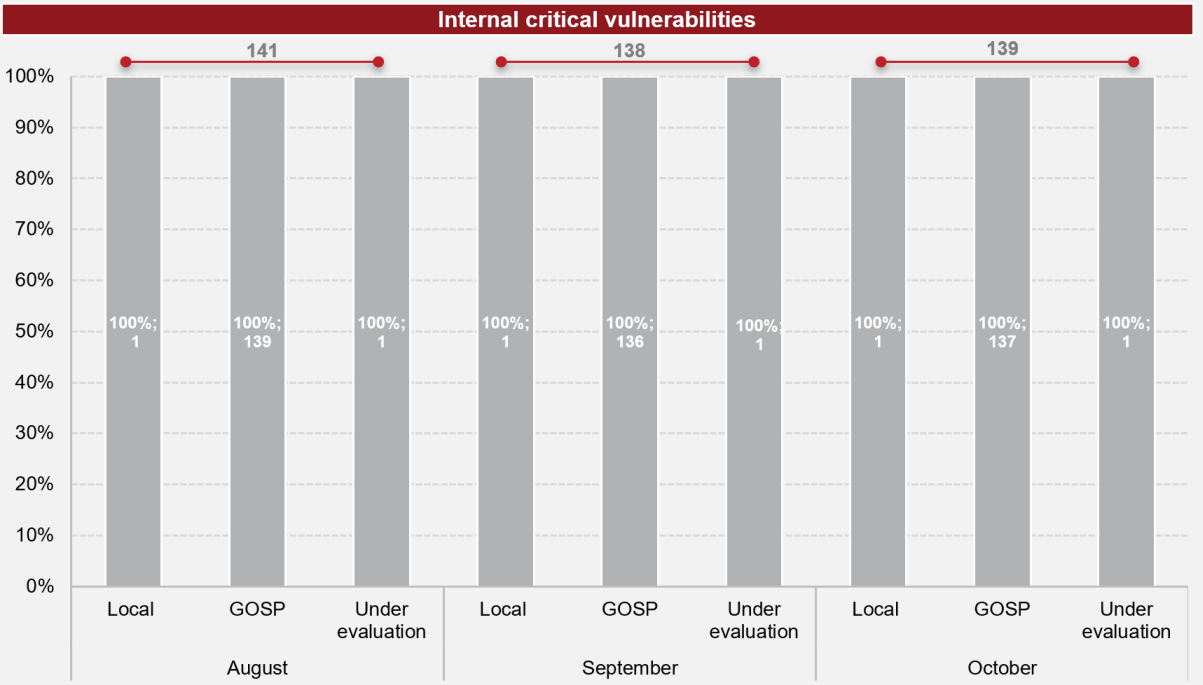
b. Classification by status

Classification by status for each perimeter, severity, and asset owner of the vulnerabilities reported in the last 3 monthly extractions. The color of the bars represents the current status.



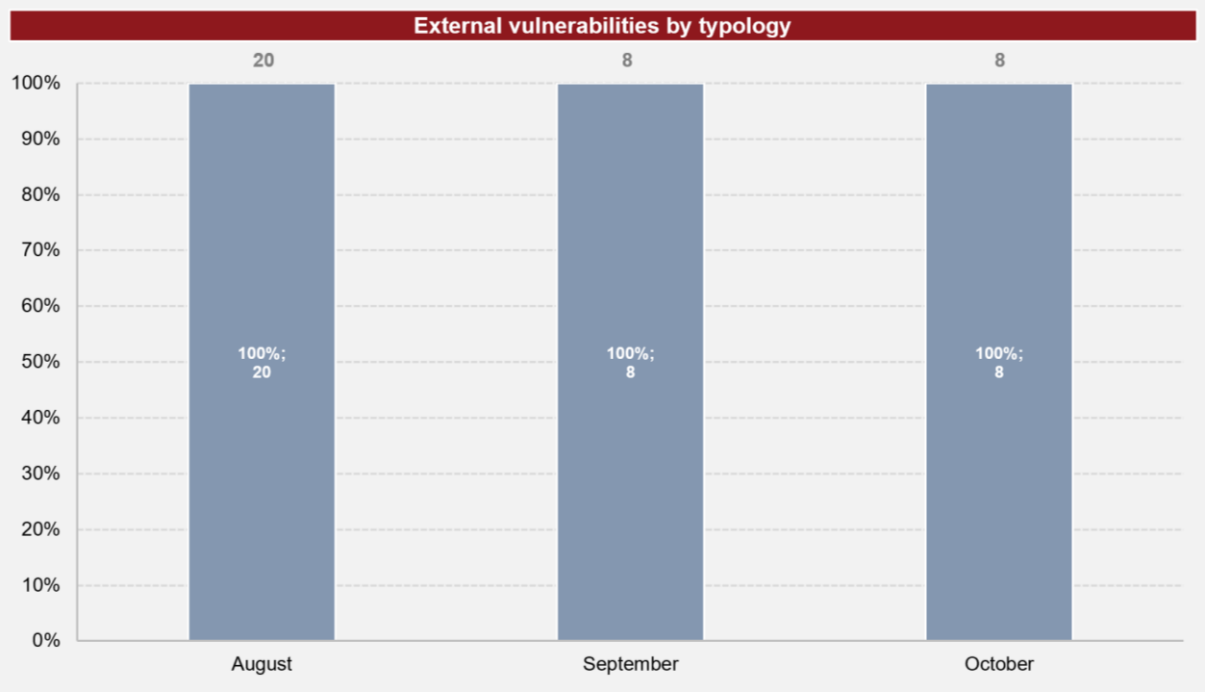


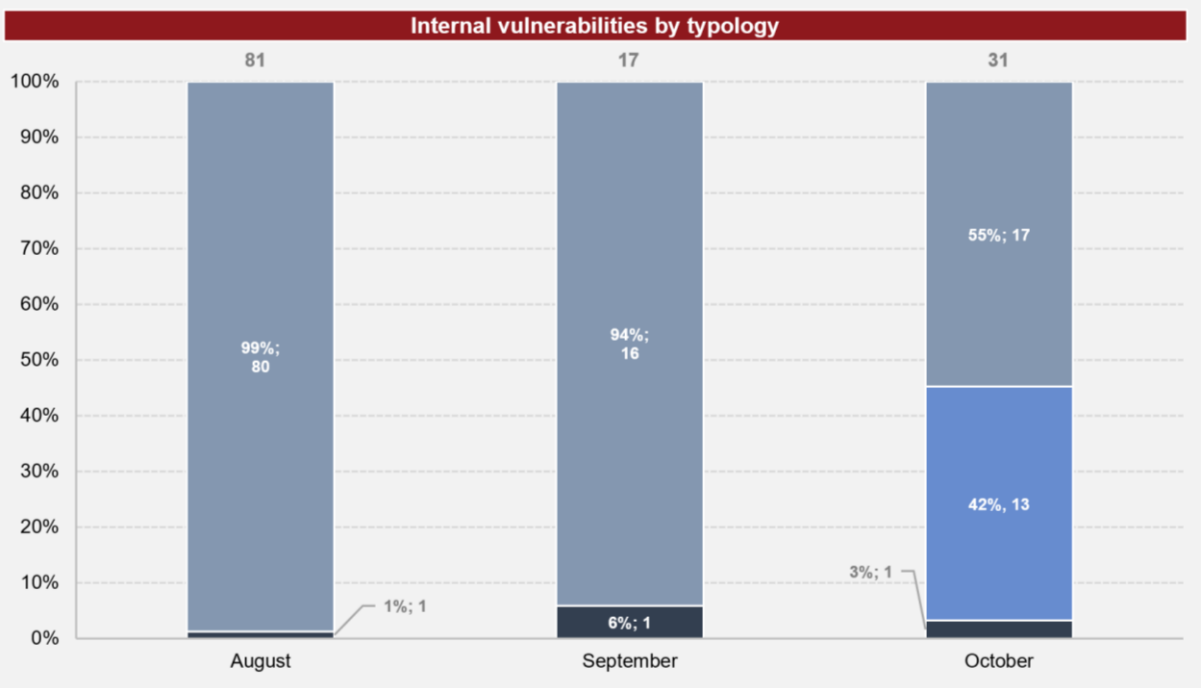

Internal high vulnerabilities
235
234
247
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
100%; 1
54%; 95
9%; 16
37%; 64
98%; 58
2%; 1
100%; 3
Pending: 1%; 2
90%; 154
5%; 8
4%; 6
98%; 60
2%; 1
100%; 2
3%; 5
Pending: 1%; 2
86%; 161
10%; 19
91%; 53
9%; 5
Local
GOSP
Under evaluation
August
September
October


Internal critical vulnerabilities
141
138
139
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
100%; 1
100%; 139
100%; 1
100%; 1
100%; 136
100%; 1
100%; 1
100%; 137
100%; 1
Local
GOSP
Under evaluation
August
September
October

c. Classification by typology

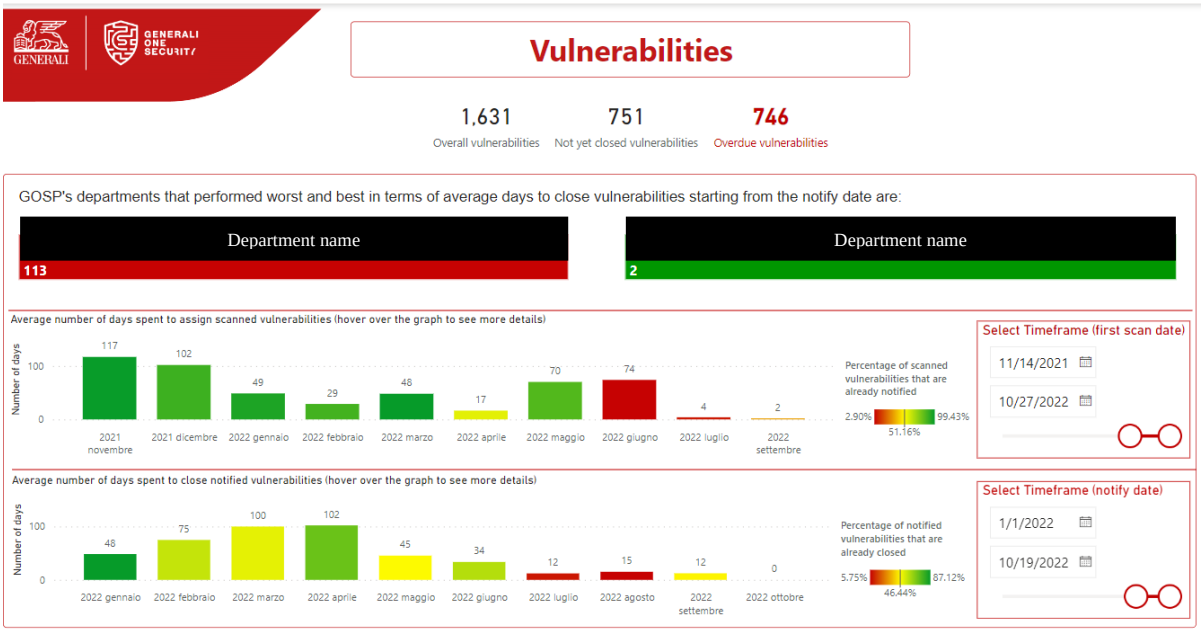
Classification for each perimeter of the vulnerabilities reported in the last 3 monthly extractions. The color of the bars represents the typology.





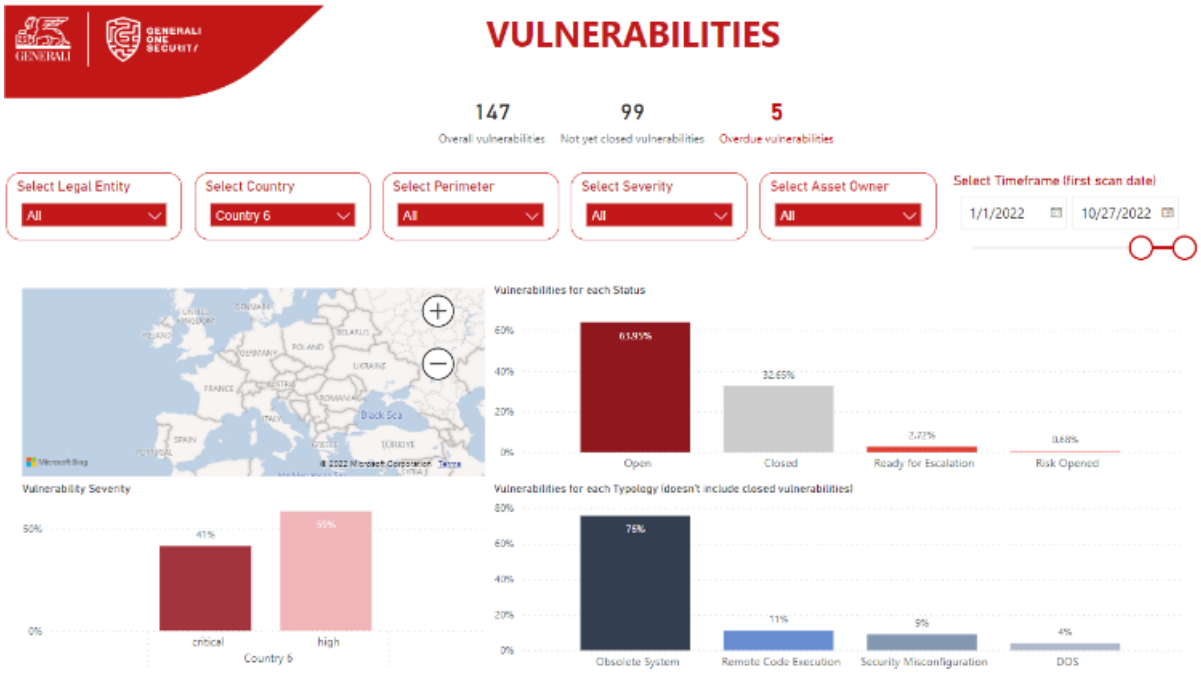
D. Dashboard

a. Summary [17]



b. Classification focus

Dashboard screen on vulnerabilities classification filtered for Country 6.



[17] The department name is confidential