Project Achilles

1st Michal Greguš
Security Analyst
CSIRT.SK
Bratislava, Slovakia
michal.gregus@csirt.sk

2nd Alexander Valach
Security Analyst
CSIRT.SK
Bratislava, Slovakia
alexander.valach@csirt.sk

3rd Marián Danko
Head of Analytical Department
CSIRT.SK
Bratislava, Slovakia
marian.danko@csirt.sk

***Abstract*—In an ever-evolving digital landscape, the role of Computer Security Incident Response Teams (CSIRTs) has become paramount in safeguarding critical infrastructure and ensuring cybersecurity compliance. In this paper, we discuss how CSIRT.SK has developed the Achilles system to fulfill its obligations and assist in protecting the team's constituency. The paper describes the design of the Achilles system, its features, and practical usage examples. It focuses on how Achilles is used at CSIRT.SK to help identify and remediate security vulnerabilities and protect the digital infrastructure of CSIRTS's constituency. Challenges encountered during the tool's development and deployment are explored along with ideas for further improvements. We hope that this article can act as an inspiration for other CSIRT teams on how security scanners can be integrated into larger systems to help manage vulnerabilities in systems belonging to their constituents.**

***Keywords*—CSIRT, Vulnerability Scanning, Nessus, NIS 2**

I. Introduction

In recent decades governments, companies, and citizens have all experienced a huge increase in the number of cyber-attacks against digital assets. Among other reasons, this can be because the threat landscape in cybersecurity is constantly evolving. As a result, the task of safeguarding critical digital infrastructure and other assets is an area of great concern for governments and company executives worldwide. To protect digital assets and critical infrastructure cybersecurity experts have created multiple standards, procedures, and directives to enhance the security posture of organizations and states. In addition to that both organizations and states have started to set up Computer Security Incident Response Teams (CSIRTs), which play a crucial role in detection, mitigation, and response to cyber threats.

In this article, we will discuss how CSIRT.SK has designed, developed, and utilized a system code-named Achilles to not only fulfill our legal obligations but also to improve the security posture of organizations in our constituency.

The rest of the paper is organized in the following way. A brief overview of laws and regulations regarding cybersecurity in the Slovak Republic along with resulting obligations for CSIRT.SK is provided in Section II. Section III covers the challenges and complexities of CSIRT.SK faced in fulfilling its legal obligations. In Section IV, we describe how the Achilles system was designed, implemented, and deployed. The next Section V describes the benefits of utilizing the Achilles system in real-world conditions along with case studies and our lessons learned. Future work and plans to improve our solution are discussed in Section VII. Finally Section VIII concludes the paper.

II. CSIRT's Legal Mandate

The EU directive 2022/2555 also known as the NIS 2 Directive is aimed at strengthening cybersecurity in the European Union [1]. In the Slovak Republic this directive has been transposed into a directive 264/2023 issued by National Security Authority (NBU) [2], [3]. Directive 264/2023 establishes the context of security measures, the content and structure of security documentation, and the scope of general security measures that shall be taken by an institution that is subject to Law number 69/2018 Z. z. on Cybersecurity [2], [4]. This law also specifies the processes of establishment and accreditation for CSIRTs.

As of now, Slovakia has three government-established CSIRT units which have been accredited by NBU [4]. These are CSIRT.MIL.SK [5], CSIRT.SK [6] and SK-CERT which is the national CSIRT unit [7]. Our unit CSIRT.SK was established within the jurisdiction of the Ministry of Investment, Regional Development and Informatics of the Slovak Republic (MIRRI SR) [8]. According to the law on Cybersecurity CSIRT.SK has to meet the accreditation conditions according to § 14 and fulfill the tasks assigned to the unit according to § 15 of Law number 69/2018 [4]. CSIRT.SK is responsible for solving cyber security incidents and performing preventive services as well as reactive services for all institutions in the public sector of the Slovak Republic. This includes more than 8,200 institutions that provide services to the citizens of the Slovak Republic [4], [9].

Law on Cybersecurity also specifies obligations for organizations in the constituency of CSIRT.SK [2], [4]. For instance, § 19, § 22, and § 24 define what measures have

to be taken by providers of basic service and digital service as well as institutions in the public sector to ensure confidentiality, integrity, and availability of digital assets [4]. Along with other items, this law mandates that entities that are subject to the law shall report specified information, data, and reports through the Unified Cyber Security Information System (the original name being Jednotný informačný systém kybernetickej bezpečnosti) [10]. For the public sector and therefore the constituency of CSIRT.SK the existing implementation is called Government Cyber Security Information System (Vládny informačný systém kybernetickej bezpečnosti, VISKB) [11].

System VISKB consists of two main components:

1) **Public component -** is accessible through a web portal for all institutions in the constituency of CSIRT.SK [12]. Each institution shall submit necessary information to the VISKB through the web portal such as contact information, a list of public internet facing IPv4, IPv6 addresses and domain names used by the institution to provide digital services to the public, information about any identified cyber security incidents on digital assets of the institution, list of all digital assets and other data. Full list of all information which shall be submitted by constituency of CSIRT.SK to the VISKB can be found here [11].
2) **Private component -** is a registry accessible only for specific institutions including accredited CSIRTs, The National Bank, Personal Data Protection Office of the Slovak Republic, NBU, and others [4]. This part of the system is intended for processing and evaluation of data and information on the state of cyber security in the public sector and is used for crisis planning in peacetime, and state management in crises outside of wartime and during wartime. It enables effective management, coordination, recording, and control of the performance of the state of systems administration in the field of cyber security for CSIRT units.

Since the deployment of the system Achilles in early 2021 institutions in the public sector from our constituency have registered tens of thousands of domain names and IP addresses, along with contact information and other necessary data to VISKB.

III. The Need for Innovation

Thanks to the system VISKB, CSIRT.SK has gained access to a centralized repository of public internet-facing IP addresses and domains belonging to organizations in our constituency. However, this information in itself provided very little additional value, in terms of being able to perform our legal obligations related to reactive incident response as well as taking proactive measures. We knew, which systems we were bound to protect, what institution they belonged to, and how to contact them, but we did not know exactly what those systems were. But more importantly, we could not determine how exposed we were to attackers nor what the attack surface of organizations in our constituency was.

Oftentimes we became aware of what particular web server or email server a constituent hosted only during the process of incident response after a security misconfiguration or well-known vulnerability with an existing patch on the server was exploited by a threat actor. Not to mention the fact that more often than we would like to admit the vulnerability exploited was the very same vulnerability that was reported by the SK-CERT or CSIRT.SK on its website in the section related to warnings and alerts about actively exploited vulnerabilities or critical vulnerabilities discovered in recent days.

During the process of incident response, we learned that in many cases the administrators of compromised systems were not even aware of the presence of critical security vulnerabilities in their systems. In other cases, they were not aware of how critical were the vulnerabilities present in their systems nor what impact exploitation of those vulnerabilities by a threat actor could have. To improve the existing state of affairs, we have decided to create a system that would enable monitoring of the presence of vulnerabilities in the systems belonging to our constituency and help remediate the identified vulnerabilities.

IV. Project Achilles

To better fulfill our legal obligations in protecting our constituents we have decided to design and implement a novel vulnerability management system, which we code-named Achilles.

This system integrates open-source software (SW) such as the Hive [13], ELK stack (Elasticsearch, Logstash, and Kibana) [14] with commercial SW primarily the Nessus vulnerability scanner [15]. The ”brain” of our Achilles system is the Cyber Operations Center (COC) see Figure 1. It consists of the several components briefly described below.

Brief description of individual components -

1) **Cyber Operation Center, COC -** is our in-house developed component in the Django framework. COC is responsible for the integration of all the other components together. It controls data transfer between different components and directs actions that other components should take through their APIs.
2) **Nessus -** is a key component of our solution. We use Nessus Professional to conduct vulnerability scans on systems belonging to our constituents. We have a customized scan configuration stored in our Nessus instance. Through an API of Nessus, COC schedules regular scans, passes target information (IPs, domain names), and also downloads scan results [15]. We have decided to utilize Nessus in our solution because it has the broadest vulnerability coverage along with the highest accuracy of all vulnerability scanning SW we considered.
3) **the Hive -** open-source incident response platform to which COC submits through an API our custom-created Portable Data Format (PDF) reports from CSV formatted Nessus scan results. We use the Hive primarily to track critical vulnerabilities identified in each organization

to be able to effectively perform their validation. The built-in emailer functionality of the Hive is then used to submit encrypted email vulnerability reports to our constituents.

4) **VISKB -** registry of all necessary information from our constituents [11], [12].
5) **ELK stack -** used to aggregate all scan results and all discovered vulnerabilities in one place. We use Kibana to create visualizations on discovered data and to perform further security analytics [14].

The combination of these components into one functioning system - Achilles with COC as the central control center allows us to greatly enhance our vulnerability monitoring and management capabilities and as a result better protect our constituents. The next section covers how our analysts use Achilles to deliver regular vulnerability reports to our constituents.

V. Achilles in Action

Since deploying Achilles in early 2021 only in the pilot phase we have been scanning 154 institutions every month. Plus we carried out additional so-called campaign scans focused on identifying the presence of newly released and actively exploited vulnerabilities on the systems in our constituency (e.g., log4shell campaign). In each scan, we scanned more than 22 000 IPs or domains. To help us make this scalable we have created a process with a series of sub-steps that covers everything from registration in VISKB to receiving a vulnerability report from system Achilles.

From Registration to Reporting

The whole process of the organization joining the Achilles system, vulnerability discovery, and reporting can be summarized by the following steps:

1) **Account Creation in VISKB** - for each of our constituents we have created an account in VISKB. Organizations then receive an invitation to VISKB that informs them about the VISKB functions along with their user data and a single-use password for the web portal.
2) **Submitting Data to VISKB** - after signing in to VISKB and changing their password representatives of our constituents submit IP addresses, domain names, contact information, and PGP public key. A full list of all data submitted to VISKB can be found here [11].
3) **Exchanging of Secrets** - after submission of necessary data we create a unique secret for each organization, which is used to encrypt vulnerability reports. This secret is uploaded to the Cyber Operations Centre and exchanged it with the contact person listed for the organization usually the CISO or an administrator of systems. Furthermore, we send each contact person an email explaining when will the scan take place and what IP address will be used by our scanner. This email is necessary for the scanned institution to be able to whitelist our scanner IP on their firewall, and also to inform their SOC team (if they have any) about the planned scanning activity.
4) **Passing Organisation Data to COC** - once we have all the necessary data in VISKB and contact personnel have been notified about our planned scanning we submit the necessary data from VISKB to our Cyber Operations Center (COC). This of course happens automatically through an Application Programming Interface (API). In COC each of the scanned organizations is listed under a unique ID. Information stored here for each organization includes: org. name, list of IP addresses and domain names, identified false positives, secret used for report encryption, and other data.
5) **Vulnerability Scanning** - each month our analysts schedule a regular monthly scan in COC. The scan is automatically started on the time and date specified by the analyst in the scheduler. Just before each scan runs latest IP address and domain data from VISKB is loaded to COC and the scan is by default run for all IPs and domains registered in COC. After the scan is finished scan results in CSV format are exported from Nessus to COC. With the current number of organizations in the Achilles system, the scan takes roughly 70 hours to complete.
6) **Report Creation** - scan results in COC are then aggregated by the organization. For each organization, a PDF vulnerability report in either a monthly or quarterly format is created. More detailed information about reports can be found in Section VI. After a PDF report is created by COC it is uploaded to the Hive where markdown notes containing names of all critical vulnerabilities identified by a combination of IP and port number for each organization are created as well. Our analysts then validate the identified critical vulnerabilities.
7) **Vulnerability Validation** - for vulnerability validation, we use other scanning software (SW), detailed description of this process is specified in Section VI. Figure 2 shows how we use the Hive to validate findings from Nessus. If a critical vulnerability is considered to be a false positive by our analysts we submit a false positive ticket to COC. Then regenerate a PDF report for the organization, removing the false positive finding from the report. Then we proceed to send the report.
8) **Sending a Report** - report is send using the emailer service built in the Hive [13]. Before the report is sent, it is of course encrypted by the secret stored in COC. It is sent to the contact email address of the CISO or system administrators listed in VISKB for each institution as the appointed point of contact for that organization.
9) **Data Visualization & Analysis** - once all the reports are sent our analysts summarize information about findings discovered in the latest scan into a report. These summarized reports are for our internal use only. More on how we utilize captured data to improve the quality and effectiveness of services provided to our constituents can be found in Section VI.

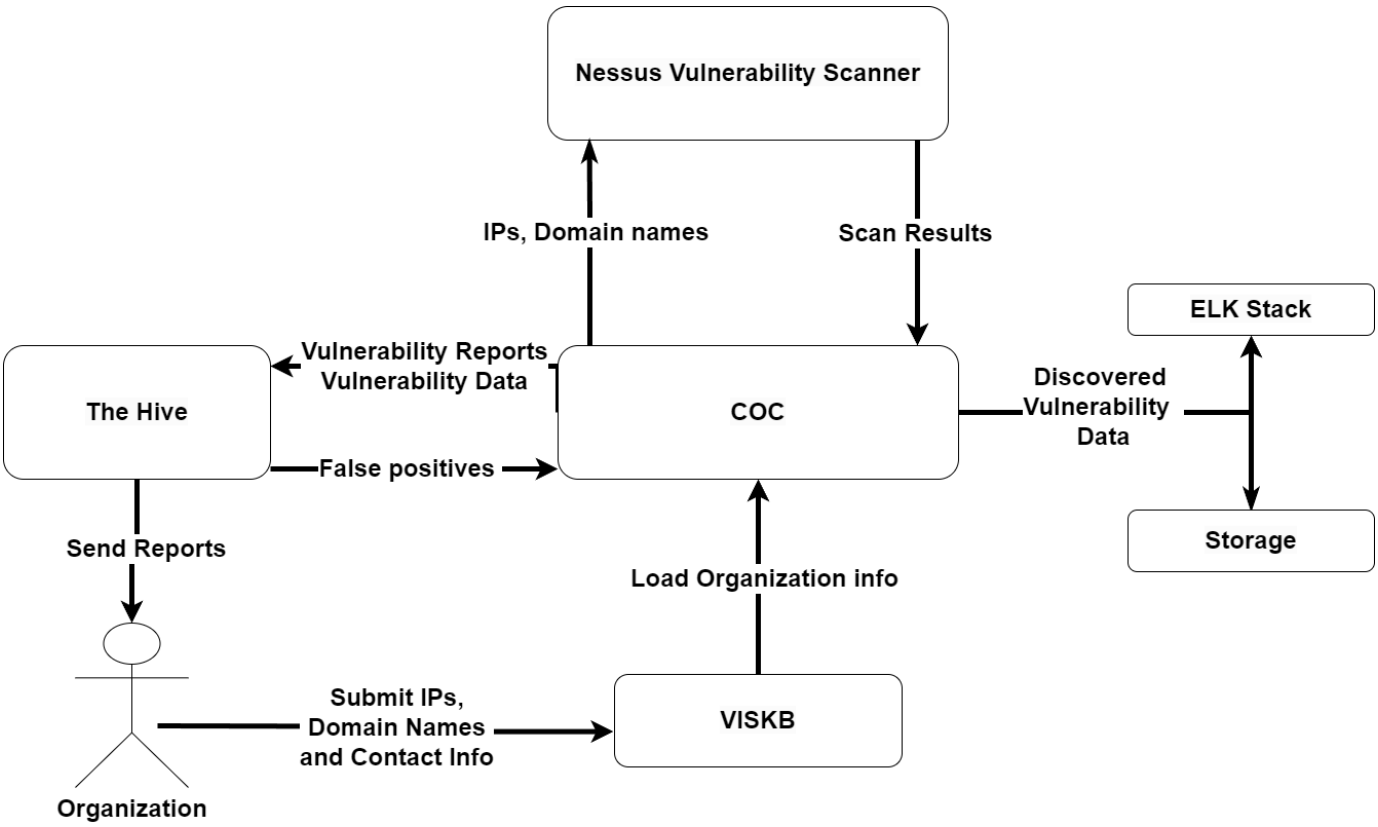

Fig. 1. The diagram depicts components that create the system Achilles.

In the future, we would like to optimize this process further. Mainly we would like to automate certain steps such as the generation of secrets and report delivery. As well as automate the process of report sending from the Hive immediately after a report is created in the Cyber Operations Center (COC).

VI. Benefits and Impact

By using the Achilles system, which is still in its pilot phase and not yet fully developed we have identified tens of thousands of vulnerabilities on the systems belonging to our constituents. Due to integration with Hive, we have managed to create hundreds of customized vulnerability reports, which we have delivered in encrypted form to contact personnel listed in VISKB from each institution. During this process, we have gained a much better understanding of the issues in front of us as well as the cybersecurity-related challenges faced by our constituents. In this section, we briefly discuss our experiences from the test phase of the project along with lessons learned and case studies.

Only in the last scan (September 2023 scan), we identified approximately 45 000 vulnerabilities with CVSS base 3 scores ranging from info to critical [16] see Table I, which contains the distribution of identified vulnerabilities based on CVSS base 3 scores. The total number of vulnerabilities with a rating high or critical is 9 471. As we have already described after running the Nessus vulnerability scan on all IPs and domains stored in COC we create PDF vulnerability reports from CSV scan results generated by Nessus.

We then load all PDF reports, one for each constituent, to the Hive along with a list of all critical vulnerabilities discovered for that given constituent. During the first year after deploying Achilles, we used specialized scanners and scripts such as nmap [17], whatweb [18], nikto [19], Joomscan [20], metasploit [21] and others to validate all critical vulnerabilities discovered by Nessus [15]. If we discovered a false positive vulnerability we submitted a ticket to COC and then regenerated a vulnerability report in the Hive to remove the false positive finding. The regenerated report was then encrypted and sent to the contact person or personnel listed by a particular constituent in VISKB.

During the whole year of validating all critical vulnerabilities, we have identified in total just 23 False Positive findings

TABLE I. Distribution of identified vulnerabilities based on their severity according to Common Vulnerability Scoring System v 3.0 (CVSS) [16]

CVSS v 3 Score	Rating	Share in Percentage
0	Info	9,51%
0.1 - 3.9	Low	1,3%
4 - 6.9	Medium	68,34%
7 - 8.9	High	9,6%
9 - 10	Critical	11,2%

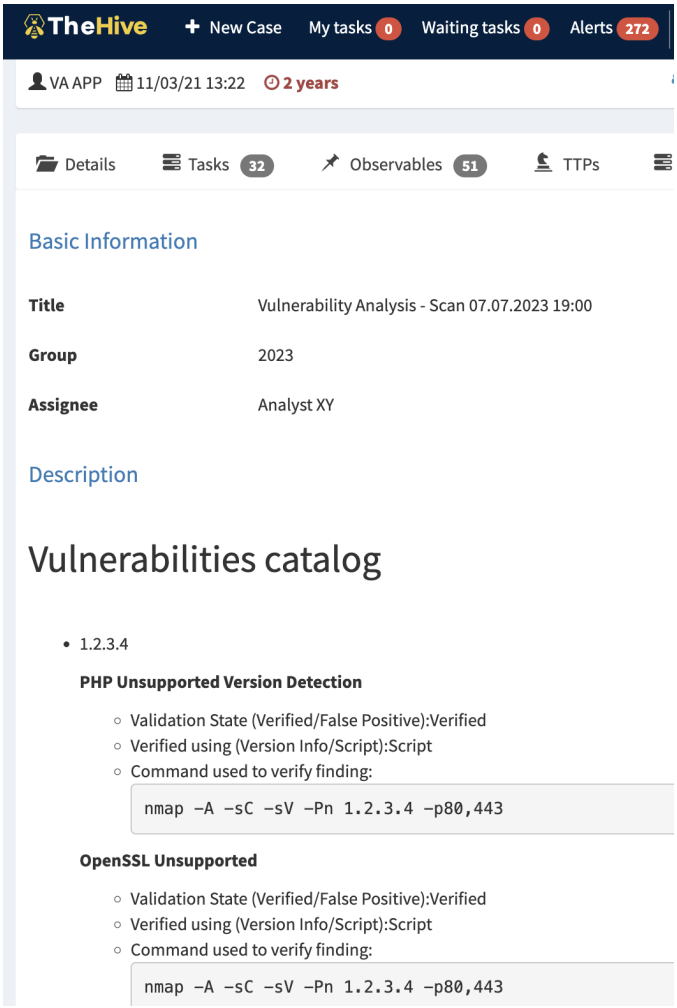

Fig. 2. Critical vulnerabilities identified on systems belonging to a particular organization sorted by host showed in the Hive. Markdown shows the command, tool, or script used to validate the finding by our analysts.

which is less than 0.1% of all critical vulnerabilities discovered over the given period. All other findings were confirmed by other specialized scanners and ergo deemed to be a True Positive finding by our analysts. This was consistent with claims made by Tenable the authors of Nessus who say that its defect rate is less than 0.32 defects per million scans thanks to its Six Sigma quality management methodology used [15]. Even though we did not expect many False Positive findings we were positively surprised by the very low rate of False Positive findings achieved.

On the other hand, what turned out to be a bit more problematic was identifying the number of False Negative findings we got. In many scenarios when using a given Nessus plugin, which determines a service version based on some self-reported information by the service such as the presence of a given HTTP header or subsite on a website simply removing this header or subsite results in the plugin's inability to identify the presence of vulnerable service running on a tested host

TABLE II. Most common services with high or critical vulnerabilities [16] provided by our constituents accessible from the internet

Service name	Share in Percentage
HTTPS	45%
HTTP	39%
SMTP	1,5%
SMTPS	0,6%
POP3S	0,6%
IMAPS	0,6%
SSH	0,5%
FTP	0,5%
DNS	0,5%
RDP	0,3%

or domain. So far we have identified a handful of cases where after the removal of the service identification header by administrators Nessus was no longer able to identify the vulnerable version of Joomla CMS even though the website was vulnerable, in addition, the vulnerability was also easily detectable when using a more specialized scanner such as Joomscan [20].

Unfortunately, at this point, we are not able to exactly quantify how many False Negative findings we get. Or to be more exact how many vulnerabilities we are not reporting because we do not discover the presence of vulnerable service running on a scanned host or domain using our Nessus scanner? This is why in the future we would like to integrate other scanning tools such as already mentioned Joomscan [20], BurpSuite [22], whatweb [18] and nikto [19] into the Achilles system, in the future.

Another benefit of deploying the Achilles system has been gaining a better understanding of the systems and services provided by our constituents to the public. Table II shows the most common services accessible from the internet running on the systems owned by our constituents. As we can see most of our constituents are only providing web services or email services to the members of the public.

In addition to this, due to passing all scan results from the Nessus scanner to ELK stack [14], we can create visualizations that help us make sense of acquired data. Thanks to using the Lens visualization feature of Kibana [14] see Figure 5, we can determine which Common Vulnerabilities and Exposures (CVEs) [23] are most prevalent in the systems owned by our constituency as presented in Figure 4. Not only that using the Lens functionality of Kibana we can create custom visualizations as can be seen in Figure 3. Among the majority of the identified critical vulnerabilities are outdated versions of Apache Web server along with old versions of PHP, as presented in Figure 3.

Moreover, we can even visualize which hosts or domains have the majority of vulnerabilities inside a given organization as can be seen in Figure 5. This allows each organization to prioritize vulnerability remediation not only based on which systems are the most vulnerable, e.g., have the most critical vulnerabilities but also based on the value of information assets

Fig. 3. Distribution of identified vulnerabilities according to CVSS rating, each category then shows the distribution of particular vulnerabilities in that category.

stored on those systems. On top of all these visualizations, Kibana also has a Dev Tools Console, which allows our analysts to query practically any possible data aggregations through a Rest API from basically all indexes stored in Elasticsearch and then conduct their own data analytics or visualizations on these data.

Another key component of our solution is website availability monitoring, which monitors all websites registered in VISKB periodically and every thirty minutes checks if the website is available. This works by sending an HTTP GET Request to all registered websites in VISKB from COC and then waiting for a corresponding HTTP GET Response. If we get a 400 or 500 error response code we increase the frequency of issued HTTP GET Requests to send one request every 4 minutes. If none of the three subsequent requests receives a successful HTTP GET Response our SOC team automatically receives an email that notifies them about the unavailability of a given website also with the time when it was last available.

This helps us identify ongoing DoS attacks on monitored websites almost in real time. According to our statistics, we are alerted about an ongoing attack by our monitoring system sooner than by responsible system administrators in 9 out of 10 DoS attacks. This allows us to further reduce incident response time as well as reduce the communication overhead necessary for members of our SOC team.

Last but certainly not least important are the PDF vulnerability reports, which are generated by COC and then sent encrypted through the Hive to contact personnel listed in VISKB for each institution. The encryption of the reports is important because most of them might contain TLP:RED classified data. Each report begins with a date and time when the scan was conducted followed by the ID of the report and the number of vulnerabilities identified.

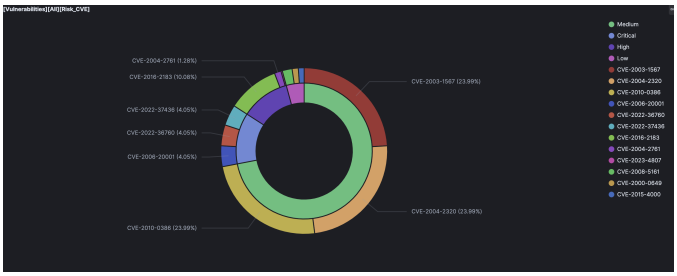

Fig. 4. Distribution of identified vulnerabilities by CVSS version 3 score, along with distribution of CVEs which are most prevalent.

After that, a brief description of the contents of the report along with a description of the process through which those vulnerabilities have been identified can be found in the report. Guidelines on how to report false positive findings back to CSIRT.SK in case any are identified by system administrators are also included.

This is then followed by a summary or a table of contents which contains all critical vulnerabilities identified and sorted by scanned host or domain. We use two kinds of report formats, a monthly variant containing only critical vulnerabilities identified and a quarterly report containing all discovered vulnerabilities along with a trend of rise or fall in the number of identified vulnerabilities on systems belonging to a given organization since we began our scanning see Figure 6.

An example of a finding from the Nessus scanner in a final report sent to an institution can be seen in Figure 7. Each finding specifies at least the name of the vulnerability, IP address, port number optionally also DNS resolution of the service on which a vulnerability was identified. This is then followed by the ID of the Nessus Plugin which was used to

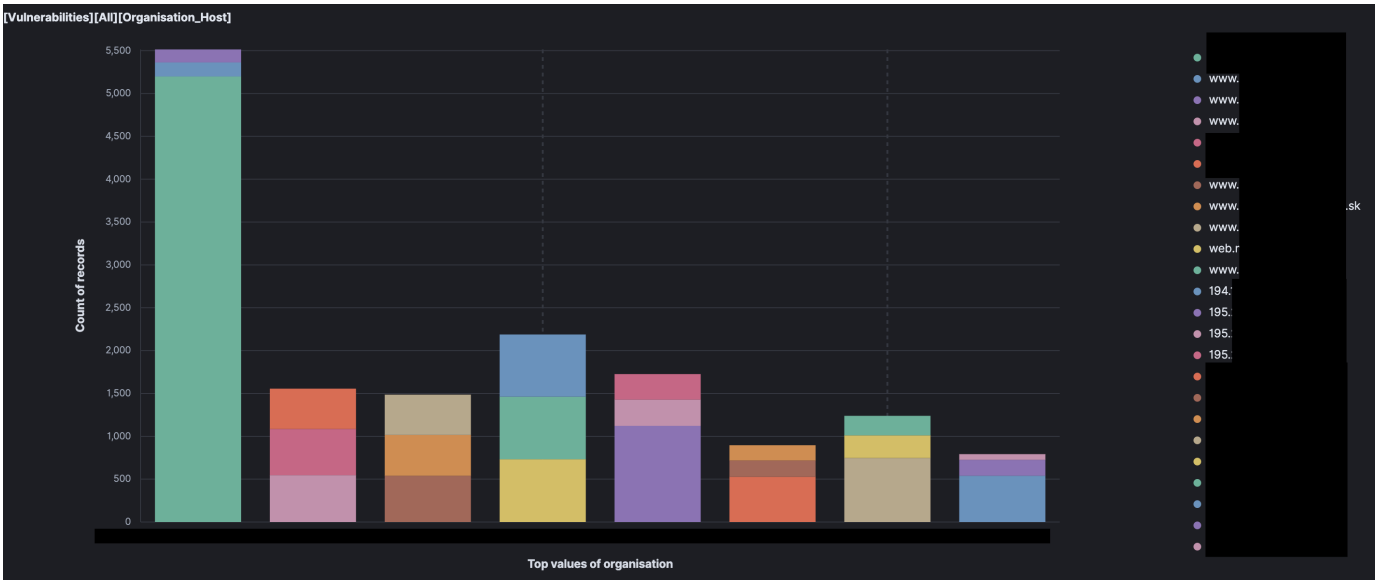

Fig. 5. Distribution of vulnerabilities by host for each organization [14].

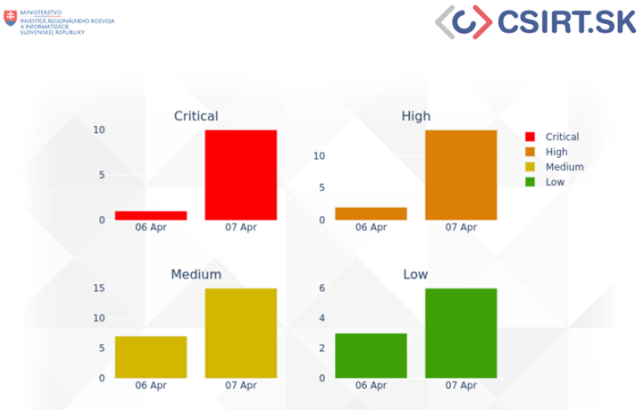

Fig. 6. Vulnerability evolution between scans - sample example.

identify the vulnerability. Also, plugin information such as Description, Synopsis, Solution or remediation recommendations, plugin references, CVSS base 3 scores, and Risk Factor of the identified vulnerability are part of the report as well.

This is to ensure that the system administrators responsible for handling the remediation of a given vulnerability not only have enough information to understand our findings and their severity but also to provide them with tips or reading materials that might aid the process of vulnerability remediation.

All this helps us improve the quality, effectiveness, and expertise of proactive measures taken by our CSIRT unit. However, it is vital to point out that results obtained from the Achilles system also help our incident response team during incident handling since they can use vulnerability reports and other data stored in the Hive to quickly identify potential attack vectors that might have been used by threat actors to compromise analyzed systems or infrastructure.

VII. Future Work

In the future, we would primarily like to focus on improving cooperation with organizations in our constituency to achieve faster remediation of identified vulnerabilities and patching of vulnerable systems. This has proved to be the main issue since the initial deployment of the Achilles system, as we in many cases still have many institutions in our constituency that have been unable to remediate critical vulnerabilities reported on their systems in more than a year.

Host informations

Vulnerability name:	Apache 2.4.x < 2.4.46 Multiple Vulnerabilities
IP:	19[redacted]
DNS:	[redacted]
Port:	80
CVE:	CVE-2020-11984, CVE-2020-11993, CVE-2020-9490
Plugin ID:	139574

Vulnerability

Synopsis:

The remote web server is affected by multiple vulnerabilities.

Description:

The version of Apache httpd installed on the remote host is prior to 2.4.46. It is, therefore, affected by multiplevulnerabilities as referenced in the 2.4.46 advisory. - Apache HTTP server 2.4.32 to 2.4.44 mod_proxy_uwsgi info

Fig. 7. Sample critical vulnerability finding from our report sent to a constituent.

To achieve this, we are planning to do regular workshops on the topic of secure administration of web servers along with the creation of supporting materials and hardening scripts. In addition to workshops related to why using HTTPS is a must in 2023. Since we have identified web server-related vulnerabilities to be the source of the majority of critical

vulnerabilities identified in our constituency. Another proactive measure taken by CSIRT.SK is providing penetration tests for newly developed web applications by organizations in our constituency before their deployment to further improve the security posture of our constituency and their resilience to cyber threats.

This should of course go hand in hand with both increasing the frequency of scanning as well as increasing the number of scanned institutions. After finishing the pilot phase of the project our goal is to scan all institutions in our constituency registered in VISKB at least every week. This means that listed contact personnel in VISKB should receive a vulnerability scan report for all their systems from CSIRT.SK weekly.

As for the Achilles system itself, future development plans include the integration of more specialized scanning SW into our solution such as BurpSuite [22], InsightVM [24] (for possible internal scans), and others. This should reduce the number of False Negative findings and potentially identify more existing vulnerabilities in already scanned systems. We would also like to make the code base of our solution open-source and available for the community, primarily the COC application.

Another issue that will require resolving in the future is IP address and domain name ownership verification. Although we try to carefully instruct each of our constituents on how to submit domain names and IP addresses to VISKB and also remind them that it is also necessary to remove them once they stop using them we have already registered cases when the wrong IP address range was submitted to VISKB or an IP address was not removed by the constituent.

These cases are particularly sensitive and we have already been asked on several occasions to explain network traffic coming from our scanner to a host belonging to an institution that did not submit the scanned IP address to VISKB. Domain ownership verification is definitely an issue that we will have to deal with in the future.

VIII. Conclusion

In this paper, we presented our solution, project Achilles, which allows us to monitor vulnerabilities in thousands of internet-facing systems of our constituents as well as inform them about discovered vulnerabilities. For this, we have used both commercial, open-source, and in-house developed software, which our development team has integrated into a functioning system code-named Achilles.

At the heart of this system is the Cyber Operations Center (COC). It loads IP address data from VISKB and then passes them to the Nessus vulnerability scanner, which allows us to discover most of the vulnerabilities existing in systems maintained by our constituents. Integration of Nessus vulnerability scan results in the Hive has allowed us to not only identify vulnerabilities in our constituent's IT systems but also inform them about these vulnerabilities as well as provide recommendations on remediating identified issues.

This helps us with the remediation of vulnerabilities in public sector IT systems reducing the attack surface of the sector as a whole. As well as improving the effectiveness of proactive actions carried out by CSIRT team members due to having access to discovered data through analytical tools such as Kibana. In the future, we would like to integrate other scanning software into the Achilles system to improve our current detection capabilities. Additionally, we would like to strengthen cooperation with our constituents to improve the processes of remediation of identified vulnerabilities.

References

[1] E. Union. "Nis2 directive." Accessed on November 1, 2023. (), [Online]. Available: https://www.nis-2-directive.com/.

[2] N. S. Authority. "Directive 264/2023 z. z." Accessed on November 1, 2023. Issued by the National Security Authority. (2023), [Online]. Available: https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2023/264/.

[3] "National security authority." Accessed on November 1, 2023, National Security Authority of the Slovak Republic. (), [Online]. Available: https://www.nbu.gov.sk/index.html.

[4] "Law on cybersecurity 69/2018 z. z." Accessed on November 1, 2023. (2018), [Online]. Available: https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2018/69/.

[5] "Military csirt." Accessed on November 1, 2023, Ministry of Defence - MIL.CSIRT.SK. (), [Online]. Available: https://csirt.mil.sk/.

[6] "Csirt slovakia." Accessed on November 1, 2023, Computer Security Incident Response Team (CSIRT) Slovakia. (), [Online]. Available: https://www.csirt.gov.sk/.

[7] "Sk-cert." Accessed on November 1, 2023, National Security Authority - SK-CERT. (), [Online]. Available: https://www.sk-cert.sk/sk/aktuality/index.html.

[8] "Ministry of investment, regional development, and informatics of the slovak republic." Accessed on November 1, 2023, Ministry of Investment, Regional Development, and Informatics of the Slovak Republic. (), [Online]. Available: https://mirri.gov.sk/en/.

[9] *Slovak statistical office*, https://slovak.statistics.sk/wps/portal/ext/Databases/administration/!ut/p/z0/04_Sj9CPykssy0xPLMnMz0vMAfIjo8ziw3wCLJycDB0NDNxMDQ0cJC/, Accessed on November 1, 2023.

[10] "Jednotný informačný systém kybernetickej bezpečnosti." Accessed on November 1, 2023, National Security Authority of the Slovak Republic. (), [Online]. Available: https://www.nbu.gov.sk/kyberneticka-bezpecnost/jednotny-informacny-system-kybernetickej-bezpecnosti/index.html.

[11] "Vládny informačný systém kybernetickej bezpečnosti - system specification." Accessed on November 1, 2023, Ministry of Investment, Regional Development, and Informatics of the Slovak Republic. (), [Online]. Available: https://mirri.gov.sk/wp-content/uploads/2018/10/Priloha-c.-3-Navrh-opisu-predmetu-zakazky.pdf.

[12] "Vládny informačný systém kybernetickej bezpečnosti - public portal." Accessed on November 1, 2023, CSIRT Slovakia. (), [Online]. Available: https://viskb.csirt.sk/.
[13] "Thehive project." Accessed on November 1, 2023. (), [Online]. Available: https://thehive-project.org/.
[14] Elastic. "Elastic Stack." Accessed on November 1, 2023. (2023), [Online]. Available: https://www.elastic.co/elastic-stack.
[15] Tenable. "Nessus." Accessed on November 1, 2023. (2023), [Online]. Available: https://www.tenable.com/products/nessus.
[16] "Cvss v3.0 specification document." Accessed on Date of Access, FIRST (Forum of Incident Response and Security Teams). (Year of access), [Online]. Available: https://www.first.org/cvss/v3.0/specification-document.
[17] Nmap Project. "Nmap - the Network Mapper." Accessed on November 1, 2023. (2023), [Online]. Available: https://nmap.org/.
[18] Urban Adventurer, *WhatWeb*, https://github.com/urbanadventurer/WhatWeb, Accessed on November 1, 2023, 2023.
[19] Sullo, *Nikto*, https://github.com/sullo/nikto, Accessed on November 1, 2023, 2023.
[20] *OWASP JoomScan*, https://github.com/OWASP/joomscan, Accessed on November 1, 2023, 2023.
[21] Metasploit. "Metasploit." Accessed on November 1, 2023. (2023), [Online]. Available: https://www.metasploit.com/.
[22] PortSwigger. "Burp Suite." Accessed on November 1, 2023. (2023), [Online]. Available: https://portswigger.net/burp.
[23] MITRE Corporation. "CVE - Common Vulnerabilities and Exposures." Accessed on November 1, 2023. (2023), [Online]. Available: https://cve.mitre.org/.
[24] *Rapid7 insightvm*, https://www.rapid7.com/products/insightvm/, Accessed: November 1, 2023.