Hindawi
Security and Communication Networks
Volume 2021, Article ID 3187205, 21 pages
https://doi.org/10.1155/2021/3187205

Review Article

Analysis and Classification of Mitigation Tools against Cyberattacks in COVID-19 Era

George Iakovakis, Constantinos-Giovanni Xarhoulacos, Konstantinos Giovas, and Dimitris Gritzalis

Information Security and Critical Infrastructure Protection (INFOSEC) Research Group Dept. of Informatics, Athens University of Economics & Business, 76 Patission Ave., Athens GR-10434, Greece

Correspondence should be addressed to Dimitris Gritzalis; dgrit@aueb.gr

Received 15 July 2021; Accepted 7 August 2021; Published 21 August 2021

Academic Editor: Konstantinos Rantos

Copyright © 2021 George Iakovakis et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

The COVID-19 outbreak has forced businesses to shift to an unprecedented "work from home" company environment. While this provides advantages for employees and businesses, it also leads to a multitude of shortcomings, most prevalent of which is the emergence of additional security risks. Previous to the outbreak, company computer networks were mainly confined within its facilities. The pandemic has now caused this network to "spread thin," as the majority of employees work remotely. This has opened up a variety of new vulnerabilities, as workers' cyber protection is not the same at home as it is in office. Although the effects of the virus are now subsiding, working remotely has embedded itself as the new normal. Thus, it is imperative for company management to take the necessary steps to ensure business continuity and be prepared to deal with an increased number of cyber threats. In our research, we provide a detailed classification for a group of tools which will facilitate risk mitigation and prevention. We also provide a selection of automated tools such as vulnerability scanners, monitoring and logging tools, and antivirus software. We outline each tool using tables, to show useful information such as advantages, disadvantages, scalability, cost, and other characteristics. Additionally, we implement decision trees for each category of tools, in an attempt to assist in navigating the large amount of information presented in this paper. Our objective is to provide a multifaceted taxonomy and analysis of mitigation tools, which will support companies in their endeavor to protect their computer networks. Our contribution can also help companies to have some type of cyber threat intelligence so as to put themselves one step ahead of cyber criminals.

1. Introduction

Within the context of computers and computer networks, an attack is any plan to expose, alter, disable, destroy, steal, or gain unauthorized access. A cyberattack is any sort of offensive maneuver that targets computer information systems, infrastructures, computer networks, or PC devices [1]. An attacker may be a person or process that attempts to access data, functions, or other restricted areas of the system without authorization, potentially with malicious intent. In terms of context, cyberattacks are often a part of cyberwarfare or cyberterrorism [2]. A cyberattack is often employed by nation-states, individuals, groups, society, or organizations and it may originate from an anonymous source.

Cyberattacks became increasingly sophisticated and menacing in the COVID-19 era. The coronavirus pandemic has challenged businesses, as they attempt to adapt to an operational and functional model which is heavily based on teleworking (working from home or other remote locations). Forcing companies to shift to a mainly digital business model has opened them up to multiple new cybersecurity risks. The reputational operational, legal, and compliance implications could be considerable if cybersecurity risks are neglected. The impact of COVID-19 on cyber risk is too high and mitigation measures, which businesses can implement, must be effective [3]. The year 2020 will be marked as a distinctively disruptive year, not only for the worldwide health crisis but also for the online life being digitally transformed, as exponential change accelerated at home and work via cyberspace [4].

A recent study held by Tanium underlined that there was a significant rise in cyberattacks due to the pandemic and that the transition to remote work led to a delay in key security projects [5]. According to ENISA [6], during the pandemic, cybercriminals have been seen fostering their capabilities, adapting quickly, and targeting relevant victim groups more effectively (Figure 1).

The increase in remote working requires expertise in cybersecurity, due to the greater exposure to cyber risk. Reports have shown that almost one in every two individuals are deceived by a phishing scam while working at home [3]. Moreover, in most cases, an attack spreads from an infected user to other employees in their organizations and half of them have been affected by ransomware within the past 12 months [7].

In this research, we will introduce a mitigation analysis of obtainable tools, which will support technical security policies. Related work is presented in section "Related Work." The main contribution of our paper is in section "Mitigation Tools Analysis and Classification" where tools are analyzed and classified in several ways. We are going to present an inventory of automated mitigation tools like vulnerability scanners, monitoring and logging tools, and antivirus software. There will be a quick outline for each tool and table, which will provide useful information such as strong and weak points, cost, and scalability. Finally, section "Conclusions" concludes with the analysis of the classification results.

2. Related Work

In an attempt to cope with the exponential rise in cyber threats, due to COVID-19, we are motivated to contribute to the research regarding cyberattack mitigation tools. Snell [8] cites utilities from specific security vendors that seek out unauthorized activity but allow safe transmissions onto the network. As described by Alzahrani et al. [9], security tools are used to scan for these widespread vulnerabilities in web applications. Moreover, their paper evaluates them based on security vulnerabilities and gives recommendations to the web applications' users and administrators aiming to educate them. The objective of Bekavac and Garbin Praničević [10] is to compare and analyze the impact of web analytics tools for measuring the performance of a business model. A summary of web analytics and metrics tools is also given, including their main characteristics, functionalities, and available types. Turuvekere and Pandit [11] focus on various attacks that are possible on a web application and compare various penetration testing tools. Naga Sudheer et al. [12] discuss the features of automated and manual testing as well as analyzing three automated software testing tools: Selenium, UFT/QTP, and Watir. This work highlights the differences between automated and manual testing. The aim of Kaur and Kumari [13] research paper is to evaluate three software testing tools to determine their usability and effectiveness. Kołtun and Pańczyk [14] help users choose the right tool, by comparing the following: Apache JMeter, LoadNinja, and Gatling. The research indicates the most important advantages and disadvantages of the selected tools.

In contrast to the aforementioned literature, our research will present a great range of IT Security tools with an extensive analysis and classification with specific criteria for the purpose of assisting users and organizations to fortify their systems.

2.1. Scope of Our Work.

The purpose of our publication is to assist in the increased treatment of computer security attack incidents through the categorization of the mitigation tools we have done. Surely, COVID-19 has played an important role in the increasing activity of malware since attackers can find a wider field to act on. As a major part of our work revolves around presenting a multitude of products and tools regarding vulnerability scanning, monitoring and logging, and AV Software, it was imperative to draw information from the most immediate source available. Thus, we extracted information from product websites and technical documents.

The work we have done can help organizations and companies effectively and efficiently protect their assets. It is critical for an organization to have a fast and effective means of responding, whenever any kind of computer security attack occurs on it or an intrusion is recognized [15]. For example, our classification can be a tool for Computer Security Incident Response Teams (CSIRTs). ENISA [16] points out how important the role of CSIRT is in dealing with security breach incidents at a national and international level. As we know the goal of the CSIRT [15]—when an incident occurs—is to control and minimize any damage, preserve evidence, provide quick and efficient recovery, prevent similar events in the future, and acquire knowledge of threats against the organization.

The results and findings of mitigation tools can help significantly in dealing with similar incidents in the future. CSIRTs concentrate on the coordination of incident handling, thereby eliminating duplication of effort. Their focus is to mitigate the potentially serious effects of a severe computer security-related problem. To achieve this goal, they concentrate their efforts on the capability to react to incidents and the resources to alert and inform its constituency, as well [17].

A best-case scenario is vulnerabilities scanner results to be shared between CSIRT for improved threat intelligence. Businesses need to support their computer security capabilities before they suffer from serious computer security problems that can harm their mission, result in significant expense, and tarnish their image [17]. The wide range of tools we suggest in our research can help significantly in this type of group. A CSIRT should also provide true business intelligence to its parent organization by virtue of the following [18]:

Information collected regarding various current and potential threats and attacks which threaten the enterprise

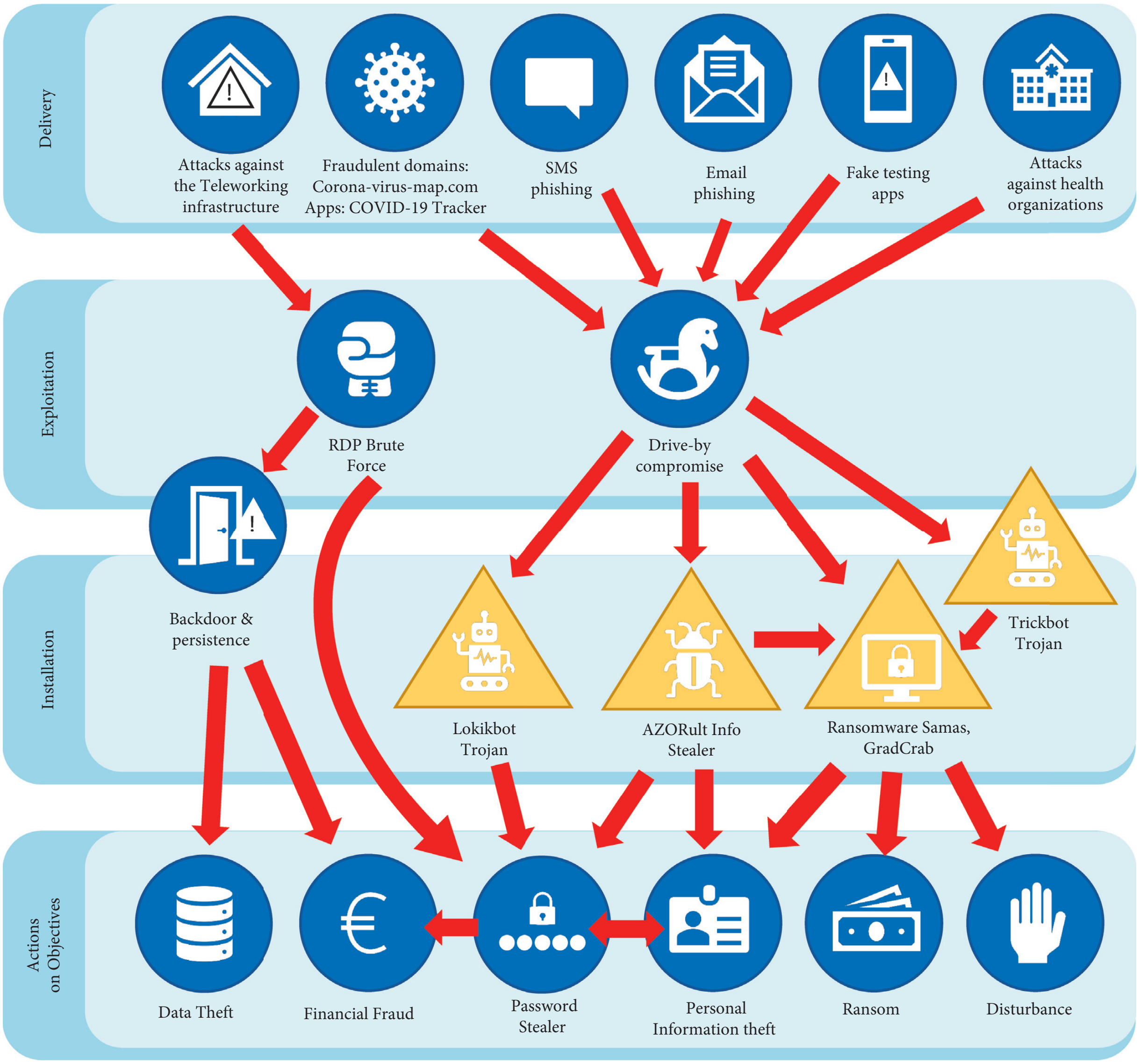

Figure 1: Threat landscape mapping during COVID-19 [6].

Knowledge of general intruder attacks, trends, and corresponding mitigation strategies

Infrastructure and policy weakness and strength comprehension: this information is based on incident postmortems

The CSIRT Network [19] provides a forum where members can cooperate, exchange information, and build trust. Members are able to discuss how to respond in a coordinated manner to specific incidents and how to handle cross-border incidents. Computer security incidents require fast and effective responses from the organizations concerned. CSIRT are responsible for receiving and reviewing incident reports and responding to them appropriately [20]. Monitoring and logging tools that have been analyzed in our survey can actually help in this direction. Additionally, threat intelligence gives organizations an edge to stay one step ahead of attackers but the threat intelligence must be relevant and coupled with the right context [21].

Analysis and classification of mitigation tools that are presented in this paper can improve threat intelligence. We mention the following benefits [22]:

Valuable insight and context: providing details on which risks are most likely to damage a company or industry, as well as indicators to help prevent and identify future attacks

Improved incident response times: prioritizing alerts allows an organization to respond faster to real threats and reduces the likelihood of significant consequences from a breach

Improved communication, planning, and investment: security teams can communicate real risks to the business and focus on defending high-risk targets from genuine threats by investing in and preparing more security

To create threat intelligence customized to information systems, CSIRTs need to collect data internally. External sources should be monitored for threat data related to any components or tools used. Tools can be utilized, which can automatically return relevant information that can provide additional context for your analyses [23]. Therefore, it is important to choose appropriate tools that will assist in the successful treatment of attacks.

Figure 2 [24] shows an indicative workflow of an incident management team. CSIRT should follow the steps while having the correct information. Our paper offers the guidelines through analysis and classification to choose the proper tools for doing this procedure.

2.2. Mitigation Tools Analysis and Classification. In this section, we present the main contribution of our paper, where mitigation tools are analyzed and classified in several ways. We aim to facilitate stakeholders to understand which tools better fit their needs. In section "Vulnerability Scanners Analysis," we analyze 25 vulnerability scanners, while in section "Classification of Vulnerability Scanners," we classify them based on 10 specific criteria. In sections "Monitoring and Logging Tools Analysis" and "Classification of Monitoring and Logging Tools," we analyze and categorize 25 monitoring and logging tools based on 8 criteria. In section "Antivirus Software Classification," we classify 14 antivirus software tools according to 9 criteria. Additionally, we implement three decisions trees for each category of tools we examined. The purpose of this paper is to give a roadmap for stakeholders (CSIRT, CISO, IT professionals, simple users, etc.), choosing the appropriate tool.

2.3. Vulnerability Scanners Analysis. A vulnerability scanner [25] is a program designed to assess computers, networks, or applications for better-known flaws. They are used for vulnerability identification and detection arising from misconfigurations or imperfect programming of a network-based quality. Their function is similar to a firewall, router, web or application server, and so on. Modern vulnerability scanners provide authenticated and unauthenticated scans. They also usually have the ability to customize vulnerability reports as well as the installed software, open ports, certificates, and other host data which will be queried as a part of their workflow. A number of them are briefly presented as follows:

(1) Acunetix: it [26] is an automated security testing tool that checks for web application vulnerabilities such as SQL Injection and Cross-site scripting. It scans websites or web applications accessible via a web browser and uses the HTTP/HTTPS protocol. Moreover, it is a tool that customizes web applications including those utilizing JavaScript, AJAX, and Web 2.0 web applications and can find almost any file.

(2) AppSpider: it [27] offers interactive reports that prioritize the highest risk and streamline remediation efforts, with links for deeper analysis. Thus, users are enabled to quickly get to and analyze the most important data. Findings are organized by attack types (XSS, SQLi, etc.) and the user can have access into a vulnerability to get more information.

(3) Apptrana: by providing services such as Application Vulnerability Scanning, Web Application Firewall (WAF), and DDos Protection, AppTrana [28] addresses the shortcomings in existing cloud security solutions. It offers comprehensive protection using only technology-based cookie cutter solutions.

(4) Arachni: it [29] aims towards helping penetration testers and administrators evaluate the web application. It is a tool that supports all major operating systems (MS Windows, Mac OS X, and Linux), and due to its integrated browser environment, it can support highly complicated web applications that make heavy use of technologies, such as JavaScript, HTML5, DOM manipulation, Ruby library, and AJAX.

(5) Burp Suite: it [30] tests Web application security. The tool has three editions: A Community Edition free of charge but with limited functionality, a Professional Edition and an Enterprise Edition that can be both purchased after a trial period. It is designed to provide a comprehensive solution for web application security checks. Besides the basic functionality, the tool has more advanced options such as a repeater, a spider, a decoder, a comparer, an extender and a sequencer. It is written in Java and developed by PortSwigger Web Security. A mobile application is also available that contains similar tools compatible with iOS 8 and above.

(6) Contrast: Contrast Security [31] is an updated security tool that has embedded code analysis and attack prevention directly into software. It protects web applications against cyberattacks. There are sensors that work actively inside applications to uncover vulnerabilities, while at the same time prevent data breaches. Contrast Protect also avoids diagnosing false positives that waste valuable time for security teams.

(7) Detectify: it [32] accomplishes automated security tests on databases, web applications and scans assets for vulnerabilities, including OWASP Top 10 and DNS misconfigurations. There is a contribution of over 150 chosen ethical hackers' security findings which are built into Detectify scanner as automated tests. At this point it should be emphasized that their submissions go beyond the known CVE libraries and this is something special for modern application security.

(8) Digifort Detect: it [33] is a three-in-one product tool. It discovers attack attempts and gives information about the time, the attacker's identity and the extent of the attack. It gathers application errors and detects security vulnerabilities an attacker could use to gain access to confidential information.

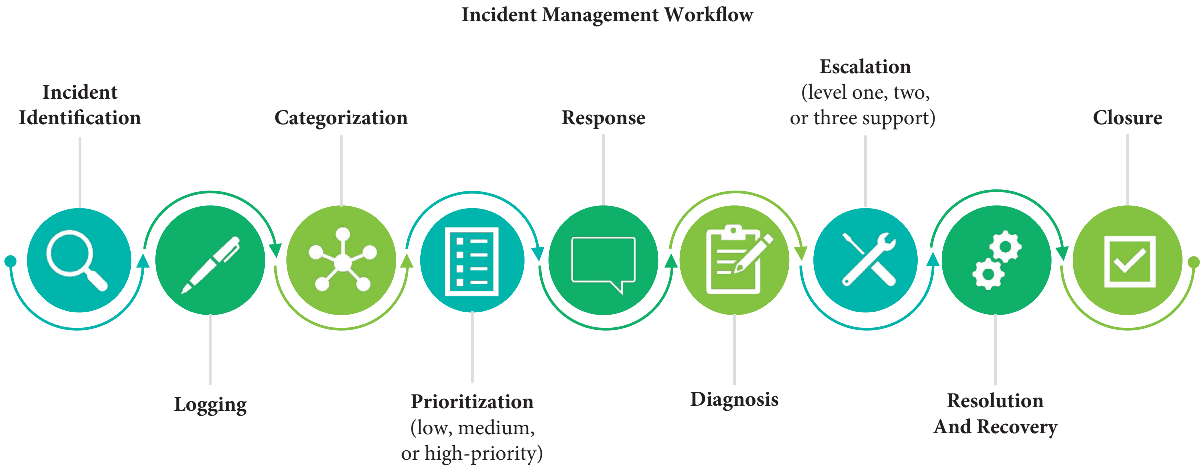
Incident Management Workflow
Incident Identification
Categorization
Response
Escalation (level one, two, or three support)
Closure
Logging
Prioritization (low, medium, or high-priority)
Diagnosis
Resolution And Recovery

Figure 2: A generic incident management workflow [24].

(9) GamaScan: it [34] is a remote online web vulnerability assessment service delivered via SaaS. The GamaSec Application Vulnerability Scanner detects not only web application weaknesses but also application vulnerabilities such as Cross-site scripting (XSS), SQL Injection, and Code Inclusion. In addition to its graphical and intuitive HTML reports, it ranks threat priority and indicates site security posture by vulnerabilities and threat exposure as well.

(10) ImmuniWeb: it [35], from Swiss firm High-Tech Bridge, is based on machine learning and artificial intelligence automation. For that reason, it has the ability to adapt to new and trending threats. It identifies the most sophisticated defects in web applications and webpages. Besides, it is claimed to detect twice as many vulnerabilities than any automated solution would. A contractual SLA for ImmuniWeb provided by High-Tech Bridge guarantees zero false positives to customers.

(11) N-Stalker: it [36] is a WebApp Security Scanner that searches for vulnerabilities, like SQL Injection, XSS, and other known attacks in web servers and web application security.

(12) Nessus: it [37] is a proprietary vulnerability scanner. It scans a wide range of technologies such as operating systems, databases, network devices, web servers, hypervisors, and critical infrastructure. Tenable Research designs programs which are called plugins to detect new vulnerabilities and are written in the Nessus Attack Scripting Language (NASL). Each plugin conveys vulnerability information and a set of remediation actions and tests for the presence of the security issue. Each week new plugins are published by Tenable, Inc., and new ones are released within 24 hours of vulnerability disclosure. In addition, this scanner haws the ability to support configuration and compliance audits, SCADA audits, and PCI compliance.

(13) NetSparker: it [38] uniquely identifies vulnerabilities such as SQL Injection and Cross-site scripting in web applications and web API, proving they are real and not false positives, once a scan is finished. It is Windows software and has an online service.

(14) Nexpose: its [39] vulnerability scanner performs various network checks for vulnerabilities. Nexpose monitors real-time vulnerabilities and acquaints itself to new hazards with fresh data. In addition, it fixes the issue based on its priority. Furthermore, Nexpose scans new devices and assesses vulnerabilities when they access the network.

(15) Nikto: it [40] is used to assess probable issues and vulnerabilities. It carries out wide-ranging tests on web servers to scan various items such as hazardous programs or files. It can scan multiple ports in one sever. Moreover, Nikto verifies the server versions whether they are outdated and checks for any specific problem that affects the server's functioning. It scans protocols such as HTTP, HTTPS, and HTTPd.

(16) OpenVas: it [41] serves as a central service that provides tools for both vulnerabilities scanning and vulnerability management. Its services are free of cost. It supports various operating systems and is licensed under GNU General Public License (GPL). It is updated with the Network Vulnerability Tests, on a regular basis.

(17) Tripwire IP360: Tripwire IP360 [42] tool is developed by Tripwire Inc. The tool can easily spot network hosts, network configurations, applications, and vulnerabilities. It also uses open standards to facilitate the risk management integration and vulnerability into multiple business processes.

(18) Retina CS: it [43] performs automated vulnerability scans for workstations, web servers, web applications, and databases providing an assessment of cross-platform vulnerability and featuring configuration compliance, patching, compliance

reporting, and so forth. In addition, it supports virtual environments such as virtual app scanning and vCenter integration.

(19) Qualys: it [44] enables organizations to achieve both vulnerability management and policy compliance initiatives cohesively. Built on top of Qualys Infrastructure and Core Services, the Qualys Clod Suite incorporates a number of applications, all of which are delivered via the Cloud: Asset view, vulnerability management, continuous monitoring, web application scanning, malware detection, policy compliance, and so forth.

(20) Probely: it [45] scans web applications to find vulnerabilities and security issues providing guidance on how to fix them. Probely performs automated security testing by integrating into Continuous Integration pipelines, following an API-First development approach, providing all features through an API. This tool covers thousands of vulnerabilities including OWASP TOP10. It is also used to check specific PCI-DSS, ISO27001, HIPAA, and GDPR requirements.

(21) Intruder: it [46] is used for scanning as soon as new vulnerabilities are released. Integrations with Slack and Jira help notify development teams when newly discovered issues need fixing, and AWS integration means IP addresses need to be synchronized to scan. It makes vulnerability management easier for small teams and for that reason it is popular among startups and medium-sized businesses.

(22) Secunia Personal Software Inspector: it [47] is mainly used to keep all the applications and programs updated and notifies users when an insecure program in a PC is being identified. It also solves security vulnerabilities.

(23) SolarWinds Network Configuration Manager: it [48] offers a vulnerability assessment feature, which claims to fix vulnerabilities using automation, as part of its Network Configuration Manager product. The software's built-in configuration manager enables users to monitor configuration changes, so as to prevent vulnerabilities. Moreover, after detecting any violations to the system, it runs automatic remediation scripts. Using this tool, users are also enabled to set continuous audit of routers and switches to monitor for compliance.

(24) Comodos Hackerproof: it [49] tests website security, by providing the daily vulnerability scanning, to ensure that no security hole exists. It has PCI scanning included and supplies a visual indicator to ensure safe transactions by the visitors.

(25) Microsoft Baseline Security Analyzer (MBSA): it is [50] a free tool of Microsoft designed to secure a Windows computer based on the specifications and guidelines set by Microsoft. It is usually used by small-sized and medium-sized organizations for managing the security of their networks. Once the scanning is done through MBSA, it presents the user with suggestions regarding fixing the vulnerabilities. It also investigates computers for any missing updates, misconfiguration, any security patches, and so forth.

2.4. Classification of Vulnerability Scanners. In this section, firstly vulnerability scanners are classified (Table 1). The tools are classified according to the following criteria: (i) strengths, (ii) weaknesses, (iii) free trial, (iv) cost/price, (v) scalability, (vi) technical support, (vii) vulnerability assessment, (viii) reports and analytics, (ix) ease of use, GUI offered, and (x) compatibility. The next part of the section includes the proposed decision tree.

Results showed that the majority of vulnerability scanners that we examined are easy to use and offer technical support, scalability, vulnerability assessment, reports, and analytics. Windows is the main operating system they support, although an adequate number of them can support most platforms. In addition, users can find free trial editions in every tool we tested, whereas only Arachni, Nikto, OpenVas, Retina CS, and Secunia, MBSA are open-source tools. The corresponding decision tree is depicted in Figure 3.

3. Monitoring and Logging Tools Analysis

Monitoring and logging tools are types of software that oversee activity and generates log files accordingly. Log files can be created by servers, application, network, and security devices. Errors, problems, and other data are continually logged and saved for analysis. In order to detect issues mechanically, system administrators, and operations, set up monitors on the generated logs. The log monitors scan the log files and explore for identified text patterns and rules that indicate necessary events. Once an event is detected, the monitoring system can send an alert, either to a specified individual or to a different software/hardware system. Monitoring logs facilitate to spot security events that occurred or may occur. A number of them will be presented as follows:

(1) Solarwinds Network Performance Monitor (NPM): Solarwinds [51] is a Windows-based tool, even though it can monitor lots of devices. A web interface provides information about the devices being monitored and helps do the configuration. Alerting and reporting are some of its features as well. Regarding general infrastructure monitoring, Solarwinds NPM fulfills that role in the Solarwinds Orion suite of tools since it provides information like availability, health status (temperature, power supply, etc.), and performance indicators (e.g., interface utilization).

(2) Solarwinds Server and Application Monitor: Solarwinds SAM [52] provides deep insight into servers and applications. The tool comes with monitoring templates, customized to monitor custom applications, so as to help get setup quickly.

Table 1: Vulnerability scanners presentation.

No.	Tool name	Strengths	Weaknesses	Free trial	Cost/price	Scalability	Technical support	Vulnerability assessment	Reports and analytics	Ease of use, GUI offered	Compatibility
1	Acunetix	Ease of use features and functionalities, quick setup with a wide range of test, network, and web vulnerability scan	Lack of AD support and static review process, does not allow web servers audit, scan may be slow when run over the internet	Yes	From 3.685€	Yes	Yes	Yes	Yes	Yes	Windows
2	AppSpider	Great job on scanning single page apps as well as APIs, no scan errors due to process failure	The UI could be better, maybe needs slightly better dashboards	Yes	By request	Yes	Yes	Yes	Yes	Yes	Windows
3	AppTrana	Quick, reliable, affordable		Yes	From 99$/ month	Yes	Yes	Yes	Yes	Yes	SaaS
4	Arachni	Ease of use, free		Yes	Free (open-source)			Yes	Yes	Yes	Most platforms supported
5	Burp Suite	Inspection/altering of HTTP requests/responses, comprehensive scans, works great on private network without Internet connection	Difficult setup for proxies, it uses tabs everywhere	Yes	From 349€/ user/year	Yes	Yes	Yes	Yes	Yes	Most platforms supported
6	Contrast	Easy to run scans, fast security results, provides security dashboard with real-time metrics	Currently supported technologies are Java, Python, and .Net, missing web layer vulnerabilities detection, e.g., detection of TLS vulnerabilities	Yes	By request	Yes	Yes	Yes	Yes	Yes	SaaS or on-premises
7	Detectify	Fully automated testing, easy to use, extremely detailed	Does not detect business logical flaws	Yes	From 40€/ user/month	Yes	Yes	Yes	Yes	Yes	SaaS
8	Digifort Inspect	Also discovers misconfigurations, lightweight, friendly		Yes	By request	Yes	Yes	Yes	Yes	Yes	SaaS
9	GamaScan	24/7 support, good dashboard, ease of use	Only Windows-based	Yes	By request	Yes	Yes	Yes	Yes	Yes	Windows
10	ImmuniWeb	Clear instructions for fixing issues, straightforward and easy to use, affordable	Does not consider business or website elements in context, does not perform advanced pen tests or brute force tests	Yes	1000$/ month	Yes	Yes	Yes	Yes	Yes	SaaS

Table 1: Continued.

No.	Tool name	Strengths	Weaknesses	Free trial	Cost/price	Scalability	Technical support	Vulnerability assessment	Reports and analytics	Ease of use, GUI offered	Compatibility
11	N-Stalker	Good support, pinpoint web application security scanner	Only windows-based	Yes	By request	Yes	Yes	Yes	Yes	Yes	Windows
12	Nessus	Easy to configure, good vulnerabilities database, good reports	Nonresponsive UI, the update of plugins takes some time	Yes	By request	Yes	Yes	Yes	Yes	Yes	Windows
13	NetSparker	Ease of use, great scanning and crawling for large and complex singe page web apps, accurate findings and coverage	Only Windows-based vulnerability handling is still a bit cumbersome	Yes	From 4.995$/year (standard edition)	Yes	Yes	Yes	Yes	Yes	Windows
14	Nexpose	Intuitive, end point agent deployment and management are easy, ease of use	Expensive, not so good filtering capabilities	Yes	From 22$/ asset	Yes	Yes	Yes	Yes	Yes	Windows/ Linux
15	Nikto	Free, ease of use	Does not find all vulnerabilities	Yes	Free (open-source)		No	Yes		Yes	Unix/Linux
16	OpenVas	Free, user-friendly, ease of use	Long time to load, not dependable as database fails often	Yes	Free (open-source)			Yes	Yes	Yes	Most platforms supported
17	Tripwire IP360	Great scalability, many support options	The ability to automate a lot of IT regulatory stuff is done well but is complex to setup	Yes	By request	Yes	Yes	Yes	Yes	Yes	Most platforms supported
18	Retina CS	Provides evaluation on the vulnerabilities found, deep analysis on networks	Sometimes the software gets stuck and runs slow	Yes	Free (open-source)			Yes		Yes	Windows
19	Qualys	Easy installation, lots of documentation, free training	Scanning areas monitored by Qualys may take long, not well suited for modern technologies	Yes	By request	Yes	Yes	Yes	Yes	Yes	Windows/ Linux
20	Probely	Full details on scan results, flexible GUI, API-driven	Limited functionality	Yes	From 69€/ month (Pro license)	Yes	Yes	Yes	Yes	Yes	SaaS
21	Intruder	Excellent support, proactive scans, ease of use		Yes	From 145€/ month (Pro license)	Yes	Yes	Yes	Yes	Yes	Most platforms supported

Table 1: Continued.

No.	Tool name	Strengths	Weaknesses	Free trial	Cost/price	Scalability	Technical support	Vulnerability assessment	Reports and analytics	Ease of use, GUI offered	Compatibility
22	Secunia Personal Software Inspector	Simple interface, ease of use, used for updating insecure applications	Takes a long time to scan for outdated programs, cannot modify the scanning schedule, often slow at scanning	Yes	Free (open-source)			Yes		Yes	Windows
23	SolarWinds Network Configuration Manager	Lightweight, easy to configure, online training	Expensive	Yes	From 2440€	Yes	Yes	Yes	Yes	Yes	Most platforms supported
24	Comodo's Hackerproof	Daily vulnerability scanning, ease of use		Yes	From 499€/ year	Yes	Yes	Yes	Yes	Yes	Most platforms supported
25	Microsoft Baseline Security Analyzer (MBSA)	Ease of use, free, good auditing tool	Does not offer in-depth security	Yes	Free (open-source)			Yes	Yes	Yes	Windows

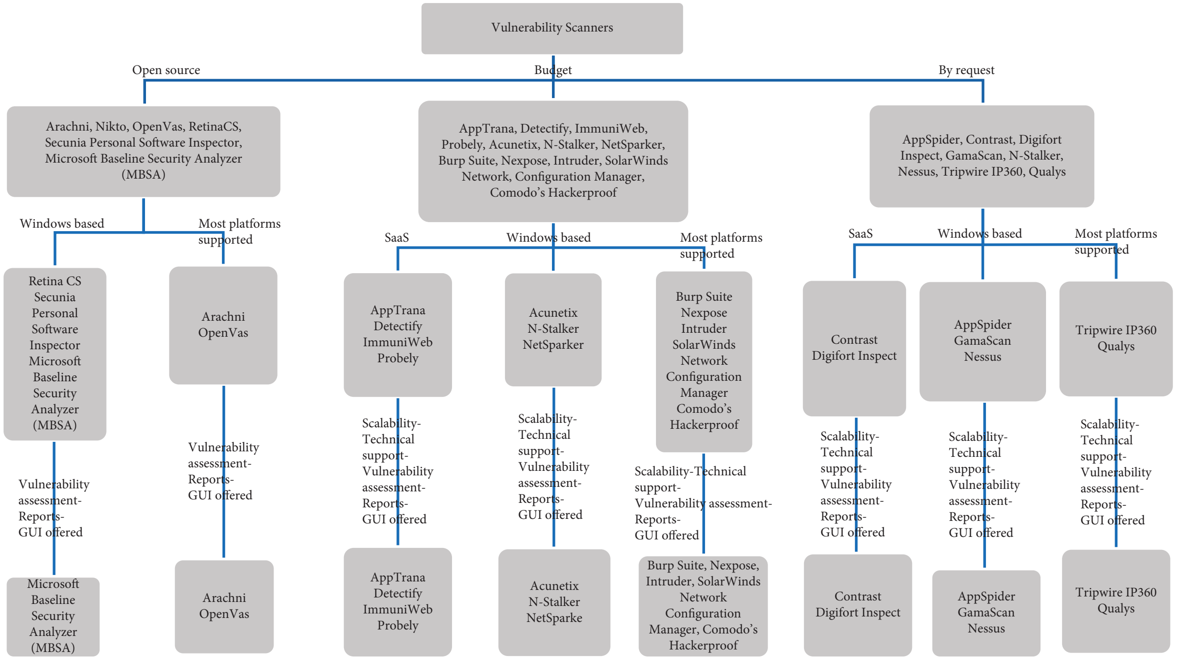
Vulnerability Scanners
Open source
Budget
By request
Arachni, Nikto, OpenVas, RetinaCS, Secunia Personal Software Inspector, Microsoft Baseline Security Analyzer (MBSA)
AppTrana, Detectify, ImmuniWeb, Probely, Acunetix, N-Stalker, NetSparker, Burp Suite, Nexpose, Intruder, SolarWinds Network, Configuration Manager, Comodo's Hackerproof
AppSpider, Contrast, Digifort Inspect, GamaScan, N-Stalker, Nessus, Tripwire IP360, Qualys
Windows based
Most platforms supported
SaaS
Windows based
Most platforms supported
SaaS
Windows based
Most platforms supported
Retina CS Secunia Personal Software Inspector Microsoft Baseline Security Analyzer (MBSA)
Arachni OpenVas
AppTrana Detectify ImmuniWeb Probely
Acunetix N-Stalker NetSparker
Burp Suite Nexpose Intruder SolarWinds Network Configuration Manager Comodo's Hackerproof
Contrast Digifort Inspect
AppSpider GamaScan Nessus
Tripwire IP360 Qualys
Vulnerability assessment- Reports- GUI offered
Vulnerability assessment- Reports- GUI offered
Scalability- Technical support- Vulnerability assessment- Reports- GUI offered
Scalability- Technical support- Vulnerability assessment- Reports- GUI offered
Scalability-Technical support- Vulnerability assessment- Reports- GUI offered
Scalability- Technical support- Vulnerability assessment- Reports- GUI offered
Scalability- Technical support- Vulnerability assessment- Reports- GUI offered
Scalability- Technical support- Vulnerability assessment- Reports- GUI offered
Microsoft Baseline Security Analyzer (MBSA)
Arachni OpenVas
AppTrana Detectify ImmuniWeb Probely
Acunetix N-Stalker NetSparke
Burp Suite, Nexpose, Intruder, SolarWinds Network Configuration Manager, Comodo's Hackerproof
Contrast Digifort Inspect
AppSpider GamaScan Nessus
Tripwire IP360 Qualys

Figure 3: Vulnerability scanners decision tree.

(3) PRTG Network Monitor: this monitoring tool is considered to be simple to set up and easy to use. PRTG [53] covers the whole monitoring spectrum, like network, bandwidth, server, and application monitoring in an all-in-one solution including, such as alerting (SMS, e-mail, Push notifications through mobile apps, etc.), robust reporting, and an intuitive web interface. It uses and relies on agentless monitoring. PRTG can be used to monitor several types of devices including Linux, Windows, Cisco, HP, and VMware; however, it can only be installed on Windows OS.

(4) WhatsUp Gold: it [54] is an easy-to-use tool that provides several features including discovery, configuration management, alerting, reporting, and monitoring of virtual environments. Some of these features are available in certain editions; WhatsUp Gold provides four different editions: Basic, Pro, Total, and Total Plus. Also, WhatsUp Gold can be installed only on Windows OS and may not be as customizable as Linux-based monitoring tools.

(5) Nagios XI: it [55] is a Linux-based solution that is flexible and powerful because the core can be extended with plugins. It comes in two types: Nagios Core, which is free and open-source, and Nagios XI, which is the paid enterprise edition. Nagios XI simplifies and makes available (by default) many of the things lacking in Nagios Core. Some of the features available on Nagios XI include a much better web interface, auto discovery, graphs, alerting (SMS, e-mail), reporting, and configuration wizards.

(6) ManageEngine OpManager: it [56] is a comprehensive IT infrastructure monitoring solution having an easy-to-use responsive web interface. It can be installed on either Windows or Linux OS and offers several features like server monitoring, network mapping, monitoring templates, alerting (SMS, e-mail), reporting network configuration management, and network traffic analysis. Most of these features are included in the base installation, whereas some require a separate license purchase.

(7) Wireshark: it [57] is a widely used network protocol analyzer. Some of this multiplatform run tool features perform live capture and offline analysis, as well as VoIP analysis. They also offer decryption support for many protocols. The output can be exported to XML, PostScript®, CSV, or plain text. Moreover, it compresses capture files with gzip and decompresses them on the spot. It is used mainly by many commercial and nonprofit enterprises, government agencies, and educational institutions and it follows a project started by Gerald Combs (1998).

(8) OP5 Monitor: it [58] is a network monitoring tool based partly on Nagios (Naemon). Some of its features include customizable dashboards, performance monitoring, alerting, reporting, web-based configuration (unlike the default Nagios Core). Moreover, it is built to scale having a license (Ent+) that can monitor over 100 K devices.

(9) Zabbix: it [59] is an all-in-one network monitoring solution. Although it supports agentless monitoring, the Zabbix server gets monitoring information from the Zabbix agent (as a client-server model). Some of the features provided by Zabbix are performance and application monitoring, web-based

configuration, auto discovery, alerting, and reporting.

(10) Icinga: it [60] is a network monitoring tool that comes in two versions: Icinga 1 and Icinga 2. Icinga provides features such as performance monitoring, alerting, reporting, extensibility through plugins. Icinga 1 resembles Nagios Core with added functionality such as a better web interface, support for more databases, and easier plugin integration. It is compatible with Nagios plugins. Icinga 2 is a rewrite of Core and features a responsive web interface. However, it reduces configuration complexity and supports distributed monitoring.

(11) LibreNMS: it [61] is a free open-source network monitoring tool and a fork of Observium. It provides features such as graphs, auto network discovery, alerting (SMS, e-mail, Slack, etc.), configuration through web interface or command-line interface. It does not have a paid support, which is available through several channels like community forums, IRC, GitHub, and Twitter.

(12) Spiceworks: its [62] inventory originally started out as a utility for scanning devices on the network and reporting information on what was running on them. It has a real-time alerting function and the community has played a significant role to its growth. Using Spiceworks Network Monitor, the user views the status of various devices and services and is alerted if particular values do not match the preset criteria.

(13) Snort: it [63] is an open-source network intrusion detection system for Linux and Windows which performs packet logging on IP networks and real-time traffic analysis. This tool is composed of two major components: a detection engine that utilizes modular plugin architecture and a flexible rule language to describe traffic to be collected. It can perform protocol analysis, content searching, and can be used to detect a variety of attacks and probes, such as stealth port scans, CGI attacks, buffer overflows, OS fingerprinting attempts, and SMB probes.

(14) Datadog: it [64] is a monitoring easy-to-install tool specially designed for hybrid cloud environments. It offers performance monitoring of network, tools, apps, and services. It can also provide extensibility through many API (Application Programming Interfaces) with documentation, graphs, metrics, and alerts, which the software can adjust dynamically based on different conditions. Moreover, the software can be downloaded and installed by agents, available for different platforms such as Windows, Mac OS, Several Linux distributions, Docker, Chef, and Puppet.

(15) ConnectWise Automate: [65] formerly known as Labtech, it can keep track of IT infrastructure devices from a single location. It discovers all devices in a network so they can be monitored proactively. The tool mitigates the issue having interpreted problems first and initiates then an automatic predefined action. Another feature is that it permits remote control, remote support, remote access, even remote meetings, by extending the ConnectWise suite. In addition, the "Patch Management" allows protection of all systems with simultaneous patching from a centralized manager.

(16) Logic Monitor: it [66] is an automated SaaS (Software-as-a-Service) IT performance monitoring tool providing full visibility of the performance and health of a network and their improvement. It discovers IT infrastructure devices and monitors them proactively, by identifying incoming issues by providing predictive alters and trend analysis. It includes a customizable dashboard, alerts, and reports.

(17) LogFusion: it [67] handles text-based log dumps, event logs, remote logging, and even remote event channels. Free and licensed versions are much of the same except for a couple of features such as customizable columns and tabbed interface.

(18) Netwrix Event Log Manager: On the freeware version, it [68] handles the basic needs such as real-time email alerting of critical events, some limited amount of alert criteria filtering, and some archiving ability (limited to 1 month).

(19) Splunk: it [69] is a log management program which encapsulates data from an entire range of devices across a network. Its core functionality can be expanded via add-ons and plugin apps. It can also work fully on-site, hybrid on-site/cloud, or fully in a cloud environment to ease remote management.

(20) Tripwire Log Center: it [70] identifies and responds to threats as well as assuring that all devices and traffic meet proper compliance and that extensive backup and protection features are on top of log management and analysis.

(21) LogRhythm: it [71] is a program that gathers log data from applications and databases from all sources. It is fully automated in a great deal of management aspect, though it is still able to be manually adjusted.

(22) SumoLogic: it [72] is a cloud-based tool that does not restrict IT professionals to the operating environment or a particular system. One of its features is that forensics are run as separate threads which can help isolate resource use in cloud space. SumoLogic does segmentation, which offers the convenience to add and remove whatever is necessary to have a customized solution for supporting your environment without wasting resources.

(23) EventTracker Log Manager: it [73] grabs all the security, application, and error logs for analysis and

encompasses Linux, Unix, Syslog, and Windows logs. It offers intuitive graphs and charts and a powerful visual front end.

(24) Correlog: it [74] focuses on the real-time management aspect. The software evaluates every bit of event information bringing to attention things of concern. It combines a centralized control interface for managing and collecting data as well.

(25) ELK Stack: ELK stands for three open-source projects: Elasticsearch, Logstash, and Kibana. Elasticsearch is a search and analytics engine. Logstash is a server-side data processing pipeline that collects data from multiple sources at the same time, transforms it, and then sends it to Elasticsearch. Kibana helps users to visualize data with charts and graphs in Elasticsearch [75]. Lately, the addition of Beats turned the stack into a four-legged project. These different components are used together for monitoring, troubleshooting, and securing IT environments (though there are many more use cases for the ELK Stack, such as business intelligence and web analytics) [76]. For many organizations, the ELK Stack is an open-source alternative to other SIEM (security information and event management) systems [77]. A CSIRT can benefit from ELK stack because of the combination of tools that it uses. Also, ELK stack can be used for vulnerability management [78].

3.1. Classification of Monitoring and Logging Tools. In Table 2, the examined tools have been classified based on the following parameters: (i) strengths, (ii) weaknesses, (iii) free trial available, (iv) cost/price, (v) scalability, (vi) technical support, (vii) reports and analytics, and (viii) ease of use, GUI offered. At the end of this section, we present the corresponding decision tree.

From the monitoring and logging tools we examined, all have free trial versions and the vast majority of them are easy to use and offer scalability, technical support, report, and analytics. Moreover, many of them like Zabbix, LibreNMS, Spiceworks, Snort, Netwrix Event Log Manager, and Splunk are open-source network systems. The decision tree is depicted in Figure 4.

3.2. Antivirus Software Classification. Commonly, malicious software is blocked by antivirus materials through the identification of code signatures distinctive to different kinds of malware. Once the applications encounter a file with a code string that matches one in their database for an already known virus, they block its access to the intended victim's computer [79].

In the fight between attackers and security researchers, the former endeavor is to break any defense mechanism by masquerading, social engineering, or by impeding antivirus software from detecting, so that they can settle on as many computers as possible and their malware can lay in the hosts for as long as possible. Installing antivirus software is often the foremost way for a user to secure his computer [80].

According to the information mentioned above, it is vital to install antivirus software. Below, there is helpful data regarding each antivirus software, which are classified using the following nine criteria: (i) strengths, (ii) weaknesses, (iii) price, (iv) on-demand malware scan, (v) on-access malware scan, (vi) website rating, (vii) malicious URL blocking, (viii) phishing protection, and (ix) behavior-based detection and the results are listed in Table 3. At the end, we present the decision tree for this category of tools.

It appears that only a few antivirus software tools are totally free of cost and these tools are Bitdefender Free Edition, Avast, Avira, and Sophos. We can also distinguish that the examined antivirus tools that meet all criteria we posed are McAfee, Symantec Norton, Webroot SecureAnywhere, Kaspersky, Trend Micro, and Bitdefender Antivirus Plus. Figure 5 depicts the decision tree.

3.3. The COVID-19 Era and Factor. In March 2020, the coronavirus was pronounced by WHO as a global pandemic. Until today (July 2021), the COVID-19 crisis has made prevention an urgent need and the lessons that humanity has learned are, hopefully, enough to highlight the serious role of IT security and privacy. The dramatic experience of COVID-19 in several countries, e.g., Brazil, India, Italy, Spain, and USA, to name a few, has outlined the importance of effective cybersecurity due to numerous successful cyberattacks. There is no surprise that, during the pandemic, more sophisticated intrusion methods were detected and reported.

Organizations must take additional steps to achieve security requirements by implementing stronger defenses and better practices. This entails applying a collection of security solutions to prevent any attraction from threat factors, as noticed during the COVID-19 pandemic and the crisis that followed. Sophisticated and highly organized cybercriminals target organizations showing every day how vulnerable the systems are. For example, health organizations have become a prime target because advanced persistent threats (APT) try to obtain information for domestic research into COVID-19-related medicine [94]. Additionally, attackers take advantage of collective fear to perform phishing campaigns using coronavirus as a trap [95]. Threat actors like hackers and state-backed attackers have been using an APT technique to gain a foothold on victim machines and launch several types of malware attacks. In 2020, e-mail phishing attacks were more than 600% since the end of February 2020 [96]. And the situation keeps getting more difficult, so there is a need of keeping one step ahead from all these intruders.

As there is no one-size-fits-all security solution, it is not feasible to address every cybersecurity challenge with a single method/technology/solution because every particular system faces different threats, different vulnerabilities, and different risk tolerances. No matter how much we shield a system, human errors and weaknesses will always be a threat. Unpredictable situations, such as the COVID-19 crisis, will create new challenges. There is an urgent need

Table 2: Monitoring and logging tools presentation.

No.	Tool name	Strengths	Weaknesses	Free trial available	Cost/price	Scalability	Technical support	Reports and analytics	Ease of use, GUI offered
1	Solarwinds Network Performance Monitor (NPM)	Easy to implement and customize, free fully functional demo, ease of scalability	Expensive, there are some user interface issues	Yes	From 2440€	Yes	Yes	Yes	Yes
2	Solarwinds Server and Application Monitor	Extensive and customizable platform, workflow that allows monitoring resources, can be integrated with open-source clients	Expensive, outdated GUI, complex architecture	Yes	From 2440€	Yes	Yes	Yes	Yes
3	PRTG Network Monitor	Very good structure and overview of your devices, ease of use and installation, very flexible	Runs only on windows	Yes	From 1200€ (PRTG500 license)	Yes	Yes	Yes	Yes
4	WhatsUp Gold	Device cards is a nice addition, easy creation of dashboard, easy GUI	Everything must be installed on-premises, device roles and discovery could use some work	Yes	By request	Yes	Yes	Yes	Yes
5	Nagios XI	Complete solution for any type of server, user interface is easy to understand and simple to customize, configuration wizards simplify the setup process	Advanced reporting should have some bulk server options, interface becomes slow when it goes to many clients in the system	Yes	From 1995$ (standard edition)	Yes	Yes	Yes	Yes
6	ManageEngine OpManager	3D visualization of the server, customizable and friendly user interface, ability to map the workflow	Everything must be installed on-premises, cloud management requires a different product	Yes	By request	Yes	Yes	Yes	Yes
7	Wireshark	Lightweight software, free, filter function, simultaneous capturing on all the network adapters	GUI should be better, might be confusing for new users	Yes	Free (open-source)		No	Yes	Yes
8	OP5 Monitor	Great support team, fast and reliable with remote collectors and load sharing	Needs work in GUI to become more user friendly, would work towards better automated tools to handle network devices	Yes	By request		Yes	Yes	Yes
9	Zabbix	Free, stores data in JSON format so other application can also use it, friendly GUI	Zabbix notification and per-user view need to be enhanced, requires lots of resources	Yes	Free (open-source)		Yes (not free)	Yes	Yes

Table 2: Continued.

No.	Tool name	Strengths	Weaknesses	Free trial available	Cost/price	Scalability	Technical support	Reports and analytics	Ease of use, GUI offered
10	Icinga	Can monitor almost everything, good community forums for support	Setup can be tricky, not so good technical support	Yes	By request	Yes	Yes	Yes	Yes
11	LibreNMS	Helpful community, free, great GUI	High memory usage	Yes	Free (open-source)	Yes	Yes	Yes	Yes
12	Spiceworks	Free, extensible with other (not free) products, good basic monitoring, easy to use and understand	The program is outdated	Yes	Free	Yes	Yes	Yes	Yes
13	Snort	Good feedback, free, network packets are saved in log file either displayed in the console	Requires significant configuration and domain knowledge to set up, sometimes gives false positives	Yes	Free	Yes	Yes	Yes	Yes
14	Datadog	Agent installation can be automated, advanced graph functionality, high level of customization	Heavy learning curve to several key features, not available as on-premises solution	Yes	Up to 31$/month	Yes	Yes	Yes	Yes
15	ConnectWise Automate	Ability to automate agent installation and manage system and vendor patch deployment, ability to offer self-service options to users, allows multiple vendors to integrate with it	Some functionality requires plug-ins, URL changes, on-premises installation requirements, complex to set up	Yes	By request	Yes	Yes	Yes	Yes
16	Logic Monitor	Agentless, comprehensive, and secure systems monitor service, excellent online help and technical support, great workflow management features	High volume of information and multiple customization options make it complex, steep learning curve for those not familiar with monitoring tools and services	Yes	By request	Yes	Yes	Yes	Yes
17	LogFusion	Lightweight, handles most of log files	Inadequate customer support	Yes	From 15$/machine	Yes	Yes	Yes	Yes
18	Netwrix Event Log Manager	Free, all event log data in a single view, ensures compliance		Yes	Free (open-source)	Yes	Yes	Yes	Yes
19	Splunk	Free, no development work required to deploy, segmentation of logs	Not free for more than the minimal use, complex until one gains experience with it	Yes	Free (open-source)	Yes	Yes	Yes	Yes
20	Tripwire Log Center	Very good monitoring, detailed reports	Reports can be more user-friendly	Yes	By request	Yes	Yes	Yes	Yes

Table 2: Continued.

No.	Tool name	Strengths	Weaknesses	Free trial available	Cost/price	Scalability	Technical support	Reports and analytics	Ease of use, GUI offered
21	LogRhythm	Excellent web console, configurable dashboards, quick searches	Not so good back-end technology, time and effort to learn how to use it properly	Yes	By request	Yes	Yes	Yes	Yes
22	SumoLogic	Good functions, log ingestion from essential any source, flexible search and reporting	Slow search for older information, poor account management, some inadequate UI decisions	Yes	From 90$/ month	Yes	Yes	Yes	Yes
23	EventTracker Log Manager	Extremely powerful search, very good support team, easy to deploy agent collectors and generate reports	Search can be complex	Yes	By request	Yes	Yes	Yes	Yes
24	Correlog	Easy deployment, good reporting	Not so good documentation	Yes	By request	Yes	Yes	Yes	Yes
25	ELK Stack	Free to get started, multiple hosting options, real-time data analysis and visualization, centralized logging capabilities	Complex management requirements, stability and uptime issues, data retention tradeoffs	Yes	Open-source	Yes	Yes	Yes	Yes

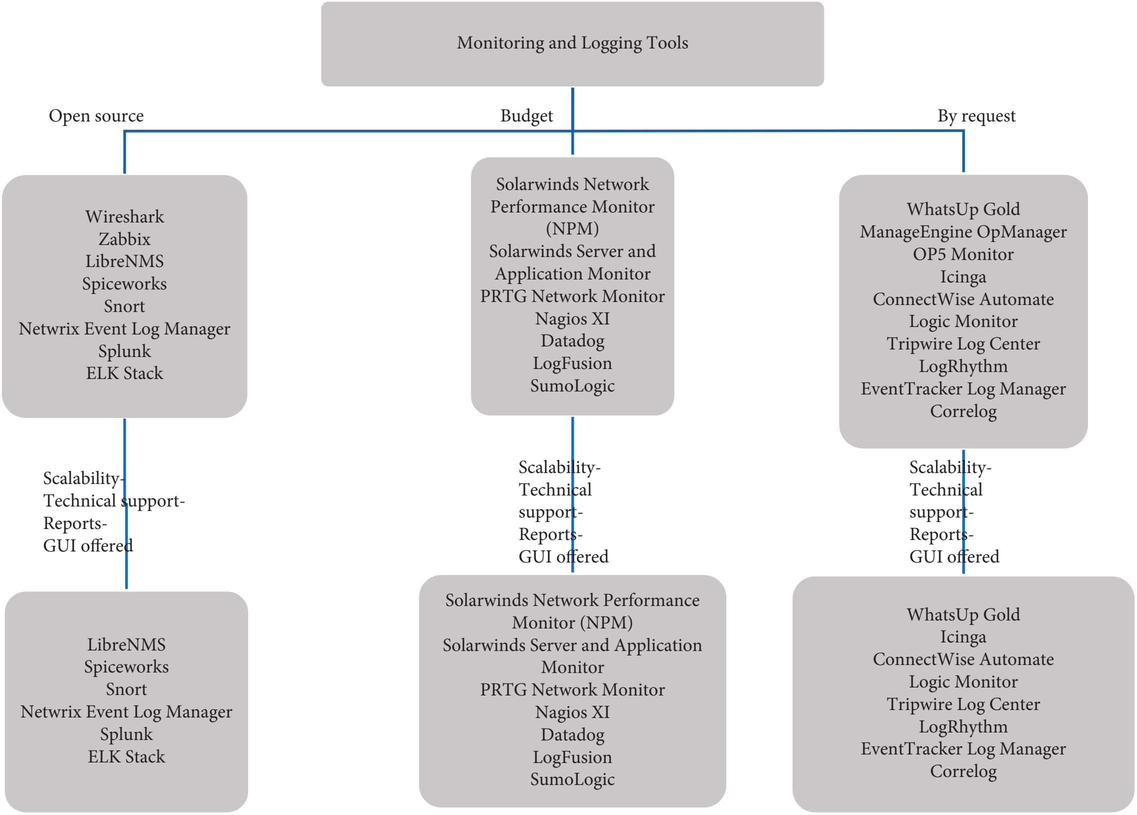

Figure 4: Monitoring and logging tools decision tree.

Table 3: Antivirus software presentation.

No.	Tool name	Strengths	Weaknesses	Price	On-demand malware scan	On-access malware scan	Website rating	Malicious URL blocking	Phishing protection	Behavior-based detection
1	McAfee AntiVirus Plus [81]	Strong protection, good scores in hands-on tests, perfect score in antiphishing tests	Fewer features in iOS, PC boost web speedup works only in Chrome	From 19.99$/ device (year)	Yes	Yes	Yes	Yes	Yes	Yes
2	Symantec Norton AntiVirus Plus [82]	Blocks even brand-new malware, low impact on system resources	Browser extension extras can be unreliable	From 39.99$/ device (year)	Yes	Yes	Yes	Yes	Yes	Yes
3	Webroot SecureAnywhere AntiVirus [83]	Extremely light on system resources, lightning fast	No testing data from the top labs	From 29.99$/ device (year)	Yes	Yes	Yes	Yes	Yes	Yes
4	Bitdefender Antivirus Plus [84]	Accurate, password manager, cheap subscription	Can be resource hungry	From 25.99$/ device (year)	Yes	Yes	Yes	Yes	Yes	Yes
5	Kaspersky AntiVirus [85]	One of the best performing security packages, supremely easy to use	Kaspersky's full suites are better value	From 39.95$/ device (year)	Yes	Yes	Yes	Yes	Yes	Yes
6	ESET NOD32 Antivirus [86]	Highly configurable, device access control	Relatively expensive, not for beginners	From 19€/ user (year)	Yes	Yes	No	Yes	Yes	Yes
7	Trend Micro Antivirus + Security [87]	Affordable pricing, easy to use, strong protection	Might slow you down, slightly limiting options		Yes	Yes	Yes	Yes	Yes	Yes
8	VoodooSoft VoodooShield [88]	Prevents nonwhitelisted programs from launching when PC is at risk, new machine-learning tool flags malware	Could possibly whitelist malware running prior to installation	From 29.99$/ device (year)	No	Yes	No	No	No	Yes
9	The Kure [89]	Exempt personal folders from being wiped, live-chat tech support built in	Malware can act freely until eliminated by reboot, does not offer 24-hour tech support	19.95$/ device (year)	No	No	No	No	No	No
10	F-Secure Antivirus [90]	User-friendly, good value	Prone to false positives	From 29.99$/ device (year)	Yes	Yes	No	Yes	No	Yes

Table 3: Continued.

No.	Tool name	Strengths	Weaknesses	Price	On-demand malware scan	On-access malware scan	Website rating	Malicious URL blocking	Phishing protection	Behavior-based detection
11	Bitdefender Antivirus Free Ed. [84]	Fast scanning, excellent virus detection	Advanced users may want more control, scans cannot be scheduled	Free	No			Yes	Yes	
12	Avast Free Antivirus [91]	Does not slow down your computer, great virus protection	Irritating privacy settings, includes links to paid-for components	Free	No	No		Yes	Yes	
13	Sophos Home [92]	Simple and nonintrusive, good cloud-based control of protected devices	No scan-scheduling, limited control for advanced users	Free	No	No		Yes	No	
14	Avira Free Antivirus [93]	Little impact on system performance, great detection rates	Little impact on system performance, lots of popups when running	Free	Yes			Yes		

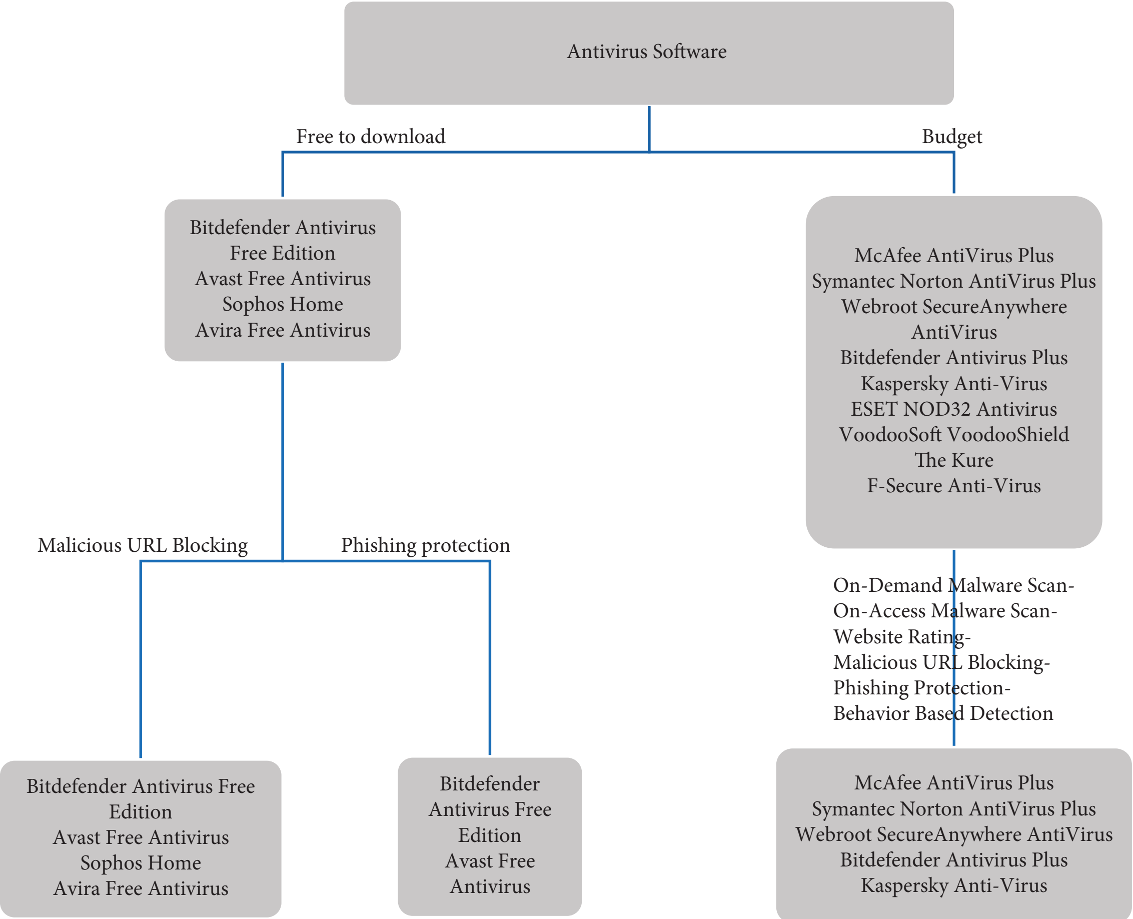

Figure 5: Antivirus software decision tree.

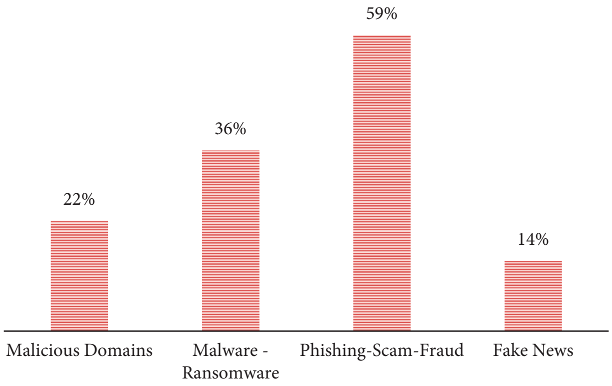

Figure 6: Interpol report-cyber threats during COVID-19.

to make protection and security measures much stronger and more effective as the risks and threats have increased. In essence, the goal of security measures is to reduce the risk of cyberattacks and data breaches. In the context of this work, we intend to propose a series of tools to IT professional or ordinary users from preventing malicious actions.

The COVID-19 situation also triggered a profound change. The crisis has resulted in the increase of various remote activities such as teleworking, remote governance, e-education, and e-commerce. Nevertheless, security and privacy management on these activities have not evolved in terms of user's awareness and cyberspace knowledge. Also, most of the security and privacy technologies available nowadays have been developed to protect the assets of systems and networks. There is a question if security solutions rise to the challenge, or there is a need to approach the problem differently [97].

Google's specialized team for threat analysis (Google's Threat Analysis Group, TAG) that works to identify new vulnerabilities and threats for its products detected 18 m malware and phishing Gmail messages, and more than 240 m spam messages related to COVID-19 daily [98]. Particularly, the TAG reported that over a dozen state-backed threat actors used COVID-19 themes as bait for phishing through emails. For example, TAG discovered a campaign that targets personal accounts of US government employees using American fast-food franchises and messages that offered free meals and coupons in response to COVID-19. By clicking on the emails, it presented phishing pages designed to trick users into providing their Google account credentials. Also, TAG found that several threat actors tried to fake users by impersonating health organizations. For example, TAG found an activity, with emails linked to a domain spoofing the World Health Organization's (WHO) login page. A similar attack was reported on MS Office 365 platform [99].

An INTERPOL impact assessment [100] related to cybercrime due to COVID-19 has shown a noticeable shift in focus, from independent personal computers or businesses to a major corporation or government networks and critical infrastructures. Criminals are taking advantage of the fact that organizations and businesses have rapidly deployed remote systems and networks to support staff working from home and the increase in security vulnerabilities, so as to steal data, generate profits, and cause disruption.

Based on the comprehensive analysis of data received from member countries and private partners, a list of cyber threats have been identified as "significant," in relation to the COVID-19 pandemic (Figure 6) [101].

As organizations of all sizes respond to the COVID-19 pandemic by allowing large numbers of employees to work from home, cybersecurity leaders face a sudden expansion of the attack surface. The remote work model, whether used temporarily in emergency situations or as a more durable solution to promote talent acquisition and business development, has also expanded its attack surface.

Managing remote workforce can be challenging because it disperses the attack surface. CISOs and sysadmins should not only pay attention to company-controlled assets, but they should also pay attention to the additional risks posed by employee personal devices that are not managed or protected by security measures from the company [102, 103].

4. Conclusions

The threat landscape has changed dramatically and new threats have arisen, due to COVID-19. This pandemic that has erupted recently has increased the number of cyberattacks worldwide. Thus, the need for security awareness and shielding of applications and information systems is essential.

The purpose of this survey was to categorize security tools which deal with threats and vulnerabilities that arise in this new era. The rationale for implementing our research was to identify the most effective tools and present them based on specific criteria so that any interested parties can benefit. Our scope is not to suggest a specific tool, but through its analysis and presentation with the use of appropriate criteria, to help stakeholders choose the right one, that is, the one that suits better to their own information systems.

Originally, the use of IT Security tools is necessary in order to maintain sufficient security for the organization. These tools help the IT department correct any misconfigurations or flaws which may have occurred and made the system vulnerable to any kind of attacks. In particular, any interested party should be aware of its risks and vulnerabilities and conduct a risk assessment. Stakeholders should invest in and use the appropriate combination of these tools which best suits their situation and with the constant and simultaneous training of its employees, it will be capable of protecting its assets.

Initially, we assessed a sufficient number of automated mitigation tools like vulnerability scanners, monitoring and logging tools, and antivirus software. We then classified these tools based on specific criteria. Furthermore, we implemented three decision trees for each category of tools we examined. We attempt to provide simple guidelines, in order to assist stakeholders (CSIRT, CISO, IT staff, simple users, etc.) in making an educated choice.

Results showed that most vulnerability scanners that we examined meet most criteria and the decision regarding which to use is ultimately based on strengths, weaknesses, cost, and compatibility with multiple platforms. A closer look at their shortcomings can help one avoid attacks on an information system. A combination of the tools can also provide better protection. With regard to the monitoring and logging tools, interested parties can select from a wide range of solutions. The analysis we made helps them decide that better suits their systems. Weighing the pros and cons and in conjunction with cost, scalability, technical support, and reports, our research can act as a guideline for reaching a decision.

As a supplementary measure against threats, we distinguish that, among the examined antivirus tools, the following meet all criteria we posed: McAfee, Symantec Norton, Webroot SecureAnywhere, Kaspersky, Trend Micro, and Bitdefender Antivirus Plus. Additionally, we could not detect evidence for Avira and Bitdefender Free Edition which proves that they could potentially meet all criteria. Users can also take into consideration the cost, as only a few are completely free of charge (Bitdefender Free Edition, Avast, Avira, Sophos).

Due to the mass effect of the COVID-19 pandemic on computer and computer network usage, the resulting cybersecurity landscape has grown exponentially in both size and complexity. Securing web applications, against evolving cyber threats, is a shared responsibility for all stakeholders. As a result, a collaborative cyber resilience model, which defines the appropriate cybersecurity posture for web applications, is quite important. Cyber threats and related risks will continue to increase, along with technological developments, which require our constant attention and vigilance.

To summarize, mitigation tools are the main ally against cyberattacks and should constantly protect and help stakeholders make prudent decisions about cyberattack protection.

Data Availability

The data used to support the findings of this study are mostly included within the article. As a major part of our scientific paper revolves around presenting a multitude of products and tools regarding vulnerability scanning, monitoring and logging, and antivirus software, it is imperative to draw information from the most immediate source available. Using that reasoning, we chose to extract information from product websites and technical documents. No online repositories were used.

Conflicts of Interest

The authors declare that they have no conflicts of interest regarding the publication of this study.

Acknowledgments

This work was supported, in part, by the Ministry of Digital Governance, Greece, through a research grant offered to the Research Center of Athens University of Economics and Business (RC/AUEB). The research aimed at, mainly, developing innovative methodologies for implementing the National Cybersecurity Strategy of Greece (2020–25).

References

[1] Csrc.nist.gov, "Cyber attack-glossary | CSRC," 2021, https://csrc.nist.gov/glossary/term/Cyber_Attack.

[2] Check Point Software, "What is a cyber attack? | check point software," 2021, https://www.checkpoint.com/cyber-hub/cyber-security/what-is-cyber-attack/.

[3] Deloitte Switzerland, "Impact of COVID-19 on cybersecurity," 2021, https://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html.

[4] D. Lohrmann, "2020: the year the COVID-19 crisis brought a cyber pandemic," 2021, https://www.govtech.com/blogs/lohrmann-on-cybersecurity/2020-the-year-the-covid-19-crisis-brought-a-cyber-pandemic.html.

[5] Security Boulevard, "90% of companies faced increased cyberattacks during COVID-19 - security boulevard," 2021, https://securityboulevard.com/2020/11/90-of-companies-faced-increased-cyberattacks-during-covid-19/.

[6] ENISA, "ENISA threat landscape report - 2020," 2021, https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends.

[7] Network Security, "Mimecast: the state of email security report 2020," 2020, https://www.mimecast.com/resources/press-releases/dates/2021/4/the-state-of-email-security-report/.

[8] M. Snell, "Tools keep Web surfing safe," *Computers & Security*, vol. 16, no. 1, p. 63, 1997.

[9] A. Alzahrani, A. Alqazzaz, N. Almashfi, H. Fu, and Y. Zhu, "Web application security tools analysis," *Studies in Media and Communication*, vol. 5, no. 2, p. 118, 2017.

[10] I. Bekavac and D. Garbin Praničević, "Web analytics tools and web metrics tools: an overview and comparative analysis," *Croatian Operational Research Review*, vol. 6, no. 2, pp. 373–386, 2015.

[11] M. Turuvekere and A. A. Pandit, "A comparative study of pen testing tools," *International Journal of Computers and Applications*, vol. 179, no. 50, pp. 26–30, 2018.

[12] B. Naga Sudheer, C. Rohan Bhadru, T. Divya Naga Paavani, and V. Lakshman Narayana, "A comparative study on automated testing tools," *Journal of Advanced Research in Dynamical and Control Systems*, vol. 12, no. 7, pp. 183–188, 2020.

[13] M. Kaur and R. Kumari, "Comparative study of automated testing tools: TestComplete and QuickTest pro,"

International Journal of Computers and Applications, vol. 24, no. 1, pp. 1–7, 2011.

[14] A. Kołtun and B. Pańczyk, “Comparative analysis of web application performance testing tools,” *Journal of Computer Sciences Institute*, vol. 17, pp. 351–357, 2020.

[15] Csirt, “Organizational Models for computer security incident response teams (CSIRT),” 2021, https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=629.

[16] Enisa.europa.eu, “ENISA maturity evaluation methodology for CSIRTs,” 2021, https://www.enisa.europa.eu/publications/study-on-csirt-maturity-evaluation-proces.

[17] Csirt.org, “Csirt,” 2021, https://www.csirt.org.

[18] Us-cert.cisa.gov, “Defining computer security incident response teams | CISA,” 2021, https://us-cert.cisa.gov/bsi/articles/best-practices/incident-management/defining-computer-security-incident-response-teams.

[19] Csirtsnetwork.eu, “CSIRTs network,” 2021, https://csirtsnetwork.eu/.

[20] Geant.org, “TF-CSIRT: computer security incident response teams - géant,” 2021, https://www.geant.org/People/Community_Programme/Task_Forces/Pages/TF-CSIRT.aspx.

[21] Security Boulevard, “Improving and automating threat intelligence for better cybersecurity,” 2021, https://securityboulevard.com/2019/12/improving-and-automating-threat-intelligence-for-better-cybersecurity/.

[22] FireEye, “the value of context: using comprehensive cyber threat intelligence to increase security effectiveness,” 2021, https://www.fireeye.com/blog/executive-perspective/2020/07/using-cyber-threat-intelligence-to-increase-security-effectiveness.html.

[23] OnPage, “How threat intelligence can improve your security - OnPage,” 2021, https://www.onpage.com/how-threat-intelligence-can-improve-your-security/.

[24] SearchITOperations, “What is IT incident management? - Definition from WhatIs.com,” 2021, https://searchitoperations.techtarget.com/definition/IT-incident-management.

[25] L. Constantin, “What are vulnerability scanners and how do they work?,” 2021, https://www.csoonline.com/article/3537230/what-are-vulnerability-scanners-and-how-do-they-work.html.

[26] Acunetix.com, “Acunetix,” 2021, https://www.acunetix.com/.

[27] Rapid7, “Web application security testing with AppSpider,” 2021, https://www.rapid7.com/products/appspider/.

[28] Indusface.com, “AppTrana,” 2021, https://apptrana.indusface.com/.

[29] Arachni-scanner.com, “Arachni - web application security scanner framework,” 2021, https://www.arachni-scanner.com/.

[30] Portswigger.net, “Burp suite - application security testing software,” 2021, https://portswigger.net/burp.

[31] Contrast security, “Contrastsecurity.com,” 2021, https://www.contrastsecurity.com.

[32] Detectify.com, “Detectifycom,” 2021, https://detectify.com/.

[33] Digifort.se, “Digifort.se,” 2021, http://www.digifort.se/en/scanner.

[34] Gamasec.com, “Gamasec.com,” 2021, http://www.gamasec.com/Gamascan.aspx.

[35] Immuniweb.com, “Immuniweb.com,” 2021, https://www.immuniweb.com/technology/.

[36] Nstalker.com, “Nstalker.com,” 2021, http://www.nstalker.com.

[37] Tenable.com, “Tenable®,” 2021, https://www.tenable.com/products/nessus.

[38] Netsparker.com, “Netsparker.com,” 2021, https://www.netsparker.com/.

[39] Rapid7.com, “Rapid7,” 2021, https://www.rapid7.com/products/nexpose/.

[40] Cirt.net, “Cirt.net,” 2021, https://cirt.net/nikto2.

[41] Openvas.org, “Openvas.org,” 2019, http://www.openvas.org/.

[42] Tripwire.com, “Tripwire.com,” 2021, https://www.tripwire.com/products/tripwire-ip360/.

[43] Beyondtrust.com, “Beyondtrustcom,” 2021, https://www.beyondtrust.com/tools/vulnerability-scanner.

[44] Qualys.com, “Qualys.com,” 2021, https://www.qualys.com/apps/web-app-scanning/.

[45] Probely.com, “Probely.com,” 2021, https://probely.com/.

[46] Intruder systems ltd, “Intruder.io,” 2021, https://intruder.io/?utm_source=referral&utm_campaign=softwaretestinghelp.

[47] Softonic.com, “Softonic,” 2021, https://secunia-personal-software-inspector.en.softonic.com.

[48] Solarwinds.com, “Solarwinds.com,” 2021, https://www.solarwinds.com/network-configuration-manager.

[49] Comodo.com, “Comodo.com,” 2021, https://www.comodo.com/hackerproof/.

[50] Microsoft.com, “Microsoft.com,” 2021, https://www.microsoft.com/en-us/download/details.aspx?id=19892.

[51] Solarwinds.com, “Solarwinds.com,” 2021, https://www.solarwinds.com/network-performance-monitor.

[52] Solarwinds.com, “Solarwinds.com,” 2021, https://www.solarwinds.com/server-application-monitor.

[53] Paessler.com, “Paessler.com,” 2021, https://www.paessler.com/prtg.

[54] “Network monitoring made easy - WhatsUp Gold,” 2021, https://www.whatsupgold.com.

[55] Nagios.com, “Nagios,” 2021, https://www.nagios.com/.

[56] Manageengine.com, “Manageengine.com,” 2021, https://www.manageengine.com/network-monitoring/index.html.

[57] Wireshark.org, “Wireshark.org,” 2021, https://www.wireshark.org/.

[58] Op5.com, “Op5.com,” 2021, https://www.op5.com/op5-monitor/.

[59] Zabbix.com, “Zabbix.com,” 2021, https://www.zabbix.com/index.

[60] Icinga.com, “Icinga,” 2021, https://icinga.com/.

[61] Librenms.org, “LibreNMS,” 2021, https://www.librenms.org/.

[62] Spiceworks.com, “Spiceworks.com,” 2021, https://www.spiceworks.com/.

[63] Snort.org, “Snort.org,” 2021, https://www.snort.org/.

[64] Datadoghq.com, “Datadoghq.com,” 2016, https://www.datadoghq.com/.

[65] Connectwise.com, “Connectwise.com,” 2021, https://www.connectwise.com/software/automate.

[66] Logicmonitor.com, “LogicMonitor,” 2021, https://www.logicmonitor.com/.

[67] Logfusion.ca, “LogFusion,” 2021, https://www.logfusion.ca/.

[68] Netwrix.com, “Netwrix.com,” 2021, https://www.netwrix.com/netwrix_event_log_manager.html.

[69] Splunk.com, “Splunk,” 2021, https://www.splunk.com/en_us/solutions/solution-areas/log-management.html.

[70] Tripwire.com, “Tripwire.com,” 2021, https://www.tripwire.com/products/tripwire-log-center/.

[71] Logrhythm.com, “Logrhythm.com,” 2021, https://www.logrhythm.com/solutions/security/log-management/.

[72] Sumologic.com, “Sumologic.com,” 2021, https://www.sumologic.com/.

[73] Eventtracker.com, “Eventtracker.com,” 2021, https://www.eventtracker.com/.

[74] Correlog.com, “Correlog.com,” 2021, https://correlog.com/download/.

[75] Elastic.co, “ELK stack: Elasticsearch, Logstash, kibana,” 2021, https://www.elastic.co/what-is/elk-stack.

[76] Logz.io, “Logz.io,” 2021, https://logz.io/learn/complete-guide-elk-stack/.

[77] Instaclustr, “Complete overview of the ELK stack,” 2021, https://www.instaclustr.com/elk-stack/#.

[78] Cloud Application Security, “Using ELK stack for vulnerability management,” 2021, https://cloudappsec.net/2018/03/18/using-elk-stack-for-vulnerability-management/.

[79] K. Heyman, “New attack tricks antivirus software,” *Computer*, vol. 40, no. 5, pp. 18–20, 2007.

[80] F. Hsu, M. Wu, C. Tso, C. Hsu, and C. Chen, “Antivirus software shield against antivirus terminators,” *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 5, pp. 1439–1447, 2012.

[81] Mcafee.com, “Mcafee.com,” 2021, https://www.mcafee.com/consumer/en-us/store/m0/index.html.

[82] Norton.com, “Norton.com,” 2021, https://us.norton.com/products/norton-360-antivirus-plus.

[83] Webroot.com, “Webroot.com,” 2021, https://www.webroot.com/us/en/home.

[84] Bitdefender.com, “Bitdefender,” 2021, https://www.bitdefender.com/solutions/antivirus.html.

[85] Kaspersky.com, “Kaspersky.com,” 2021, https://www.kaspersky.com/antivirus.

[86] Eset.com, “Eset.com,” 2021, https://www.eset.com/gr-en/home/antivirus/.

[87] Trendmicro.com, “Trend Micro,” 2021, https://www.trendmicro.com/en_us/forHome/products/antivirus-plus.html.

[88] Voodooshield.com, “Voodooshield.com,” 2021, https://voodooshield.com/.

[89] The kure, “Thekure.com,” 2021, https://thekure.com/.

[90] F-secure com, “F-secure.com,” 2021, https://www.f-secure.com/en/home/products/anti-virus.

[91] Bitdefender.com, “Bitdefender,” 2021, https://www.bitdefender.com/solutions/free.html.

[92] Avast.com, “Avast.com,” 2021, https://www.avast.com/index.

[93] Sophos.com, “Sophos.com,” 2021, https://home.sophos.com/en-us.aspx.

[94] Avira.com, “Avira,” 2021, https://www.avira.com/en/free-antivirus-windows.

[95] Cybersecurity and Infrastructure Security Agency (Cisa), “COVID-19 exploited by malicious cyber actors,” 2020, https://www.us-cert.gov/ncas/alerts/aa20-099a.

[96] Malwarebytes, “APTs and COVID-19: how advanced persistent threats use the coronavirus as a lure,” 2021, https://blog.malwarebytes.com/threat-analysis/2020/04/apts-and-covid-19-how-advanced-persistent-threats-use-the-coronavirus-as-a-lure/.

[97] R. Kunwar and P. Sharma, “Social media: a new vector for cyber attack,” in *Proceedings of the 2016 International Conference on Advances in Computing, Communication, & Automation (ICACCA) (Spring)*, pp. 1–5, Dehradun, India, April 2016.

[98] ghost-iot.eu, “GHOST: a user-friendly application to improve security and privacy,” 2020, https://www.ghost-iot.eu/ghost-project.

[99] S. Huntley, “Findings on COVID-19 and online security threats,” 2020, https://blog.google/technology/safety-security/threat-analysis-group/findings-covid-19-and-online-security-threats/.

[100] Abnormal Security, “Abnormal attack stories: WHO impersonation,” 2020, https://abnormalsecurity.com/blog/abnormal-attack-stories-who-impersonation/.

[101] Interpol.int, “INTERPOL report shows alarming rate of cyberattacks during COVID-19,” 2021, https://www.interpol.int/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19.

[102] Interpol, *Cybercrime: COVID-19 Analysis Report*, Interpol, Lyon, France, 2020.

[103] Tenable®, “How COVID-19 response is expanding the cyberattack surface,” 2021, https://www.tenable.com/blog/how-covid-19-response-is-expanding-the-cyberattack-surface.