IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 10, Issue 8, August 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.569

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 8, August 2021 ||

| DOI:10.15680/IJIRSET.2021.1008157 |

Cyber Security Threats: Attacks, Challenges & Solutions

Deepak Mallikarjun Yadav[1], Rupesh Subhash Jadhav[2]

U.G. Student, Department of Information Technology, B. K. Birla College of Arts, Science & Commerce (Autonomous), Kalyan, Maharashtra, India[1]

U.G. Student, Department of Information Technology, B. K. Birla College of Arts, Science & Commerce (Autonomous), Kalyan, Maharashtra, India[2]

ABSTRACT: There has been a huge increase in research in the area of cyber security to support cyber applications and prevent security threats against these systems. The purpose of this study is to identify and analyze common cyber security threats. To achieve this goal, a systematic approach was developed, and in total, 25 primary studies were conducted identified, and analyzed. After a detailed analysis of the selected studies, we identified the key safety threats and their frequency of occurrence. The information was also compiled and analyzed to present the publication site, the country was the publication was highly targeted infrastructure and usage. The results show that the safety measures mentioned so far only security are generally targeted, and the remedies proposed in these studies need to be thoroughly validated and implemented. Moreover, our findings show that the majority of the subjects selected in this article aim for handful common security concerns threats such as identity theft and cyber-attacks. However, there is a must to be cautious be identified important cyber-threats, targeted/harassed applications, mitigation solutions, and infrastructure over them and the challenges facing an existing province, so that scholars and interpreter can collaborate will be able to obtain a better comprehension thereof.

KEYWORDS: Threats, Attacks, Cyber security, cybercriminals, report.

I. INTRODUCTION

The World Health Organization announced COVID-19 for the outbreak in Wuhan, China in 2020. Diseases have adversely affected the world's economy and existence. [1] Many countries round the world have imposed restrictions on travel, keys, and public transportation. Within the current context of the system, Information and Engineering plays a crucial role in human communication. Most educational institutions use online platforms, where students and staff work from home. Additionally, these businesses, health care emails, food delivery, and online shopping have seen an excellent need. Cruel attackers may view COVID-19 as a chance to launch an attack on gain and further their evil intentions. The character and severity of those attacks increase over time. At present, many companies and nations are put at risk thanks to an absence of awareness of the various kinds of assaults, their ubiquity, and their limited sharpness. Developing appropriate security measures requires an intensive understanding of such attacks and their isolation. Thus a good range of cyberattacks and segmentation attacks form an integral a part of cyber security programs. The study attempts to differentiate attacks supported various factors like severity, purpose, legitimacy to produce insight into the motive for these attacks which will allow program planners to develop safety features and procedures on the idea of the attack process. The study attempts to differentiate attacks supported various factors like sharpness, purpose, legitimacy to provide insight into the motive for that attack that might allow system planners to enhance security devices and processes on the idea of attack mode. This paper tries to convey an inspiration of the assorted attack styles, there are basic methods and solutions under them under and also mentioned the references we employed in this research.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 8, August 2021 ||

| DOI:10.15680/IJIRSET.2021.1008157 |

WHAT CYBER SECURITY THREATS ARE?

The cyber security threat refers to any malicious attack that could otherwise infringe on the data, disrupt digital operations, or damaged data as per crime cost growth fig (a).

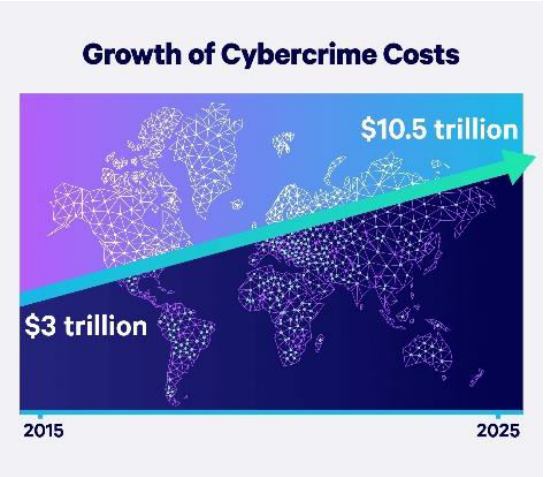

Figure (a). Rising Costs of Cyberwarfare.

Many cyber-attacks have led to the emergence of sensitive data. For example, violations of 2017 Equifax endanger the personal data of nearly 143 million consumers, including birthdays, addresses, and Social Security numbers. In 2018, Marriott International [2] revealed that hackers had access to the company's servers and stole the information of about 500 million customers. In this instance, the organization's failure to use, test, and re-test technological protections such as encryption, authentication, and firewalls exacerbates the cyber security threat. Cybercriminals can use sensitive personal or corporate data to steal information or gain access to their financial accounts, among other things that can be harmful, which is why cyber security experts are important to keep your personal information safe.

II. POPULAR ATTACKS

There are many attacks which were taking place in the world, here we listed some out of them which are common and that much important too.

1. **Ransomware attack:**
   Hackers lock the personal computer and access all the information from computers for demanding money and blackmailing. The attacks through an initial social engineering attack or exploiting a weakness in the system, the malicious ransomware software is installed on a system and then waits for a signal to begin for encrypting all the files and data which can unreadable to the owner, [10] the ransomware does this by using an encryption algorithm like AES or RSA to encrypt every file it can and the key to decrypting all of the files is in the hands of the attackers. The attackers demand money in the form of bitcoins as per record the annual damage due to Ransomware attacks fig (b).

Figure (b). Annual Ransomware Damage.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 8, August 2021 ||

| DOI:10.15680/IJIRSET.2021.1008157 |

2. WannaCry attack:

The WannaCry attacks asked for around 0.1 Bitcoin i.e. $300 and gave the user 3 days to pay money after 3 days the money gets doubled, for another 3 days, and then the data was gone.

In last year,[10] the WannaCry had infected over 200,000 device systems like Windows XP were particularly vulnerable as no correct patch was available at that time to protect them. The most of the infected device was running on windows 7 and they were vulnerable and infected because of WannaCry's ability to spread easily and rapidly through local networks.

The NHS (National Health Services of Britain) was one of the worst infected organizations around the globe and this attack caused them around $100M. As a single of students from England, he was studying cyberspace safety and he began to search on WannaCry attack and he discovered a URL in the code for the unregistered domain.

(Domain – IUQERFSODP9IFJAPOSDFJHGOSURIJFAEWRWERGWEA.COM)

That boy quickly registers the domain himself and after that, the infection rate of attack suddenly and rapidly started to drop. Later it was found that this domain was a "kill chain".

3. NotPetya attack:

According to a security expert, the NotPetya is made to spread quickly and cause damage with a single hit possibly a debatable cover of ransomware, [3] NotPetya is malware, not Ransomware, by the cyber security company Lucideus, the goal of this malware is purely evil and its motive is not to make money but to destroy data, it will simply destroy your file on the computer. NotPetya's primary target is businesses, this means that it can spread across the networks. This malware has infected the private terminal operated by Maersk at Jawaharlal Nehru trust and major businesses in Europe, US and Asia. The affected businesses include France saint Gobain, Russian Evraz, and Rosneft.

For avoiding this, you have to update your computer regularly or you can create a "perfc.dat "file in your windows folder with read-only mode. So it stops the malware from deleting your files.

4. Phishing attack:

The term Phishing with a pH is a spin on the word phishing because attackers are hanging a fake attraction of a legitimate-looking email, website, or ad, hoping the users will bite by providing the information. The attackers have requested such as a credit card number, account number, user names, passwords, and other important information, they frequently carried out by adding the link on the quote phishing messages that appears to take you to the business's website to fill in your website information but the website is a fake and the information you provide goes straight to the skew – whiff behind the scam.

The phishing technique continues to find various and fresh approaches to avail vulnerabilities like sites as fig (c) beside this there are some phishing techniques like email phishing which is the more popular widely well-known form of phishing attack is an attempt to gain access to your personal information an email that sums to be from a legitimate group. The second technique such as malware phishing uses the same technique as email phishing but this attack encourages targets to click a link or download an attachment, so some way virus can be installed on your devices.

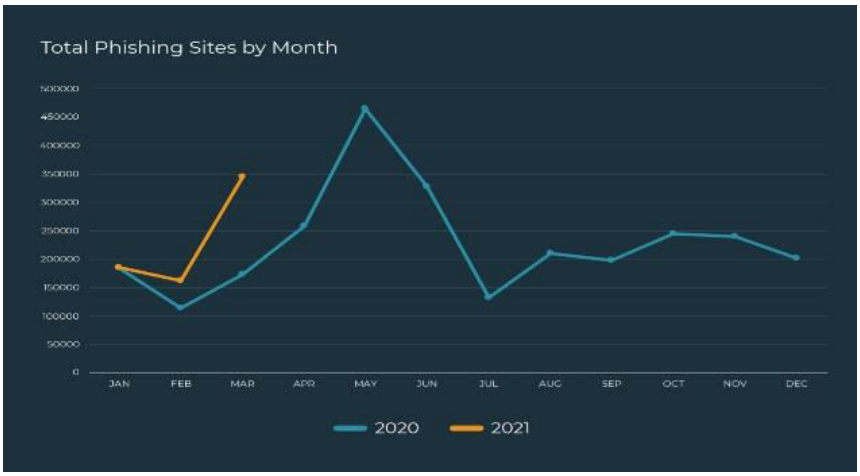

Figure (c). Phishing Attacks.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 8, August 2021 ||

| DOI:10.15680/IJIRSET.2021.1008157 |

III. REASONS OF ATTACKS

There are many causes for assaults in any organization, workplace, or on a personal level, but some of the more prevalent and essential ones are given here:

- One of the common reasons for attacks on devices is that the lack of regular updating in the system and number of systems are running on older versions due to that their security patch update isn't installed[4].
- Due to vulnerabilities in the system, [4] the attackers easily access and implanted the logic bombs, retina images, etc. so they can breach into the system.
- There are millions of unsecured codes which may not be fully secured are squeezed by cybercriminals and they see the opportunity to go through the computer.
- The users are attracted by some cookies or websites, via mail which causes them into trouble due to the negligence attitude towards the safety of computers.

IV. CHALLENGES IN EXISTING STATE

- The 5G network [8] is something that makes young people want to know more. This is because it will allow the current generation to use their favourite gadgets very well. But here's the problem - the next generation will be the victims of emotional or physical abuse. Such attacks will come from the side of cyber attackers who will illegally enter 5G wireless networks that contain complex structures at various points and misuse the data collected or stored by smart plus speed tools. Those attackers could be third parties who, by their dynamic marketing strategies, have suffocated the communications department. With the increased demand for M2M connection, the 5G infrastructure market might reach 47.775 million US dollars by 2027. As a result, it's critical to track down the identities of third-party hackers who are on a never-ending quest to gain illegal access to user data and, as a result, violate privacy and confidence in the business sector.

- Artificial Intelligence-enabled tools are now being used by the healthcare industry and resource departments. Additionally, those technologies offer specific machine learning and natural language processing (NLP) characteristics that aid in the control of data sets that are largely involved in patient information or orders involving vendors/distributors. More than 25% of health-care firms, according to a McKinsey survey, are investing in AI tools in this age-old COVID. More than 30% of analytics available through AI / ML techniques are used in the banking industry. fig (d)

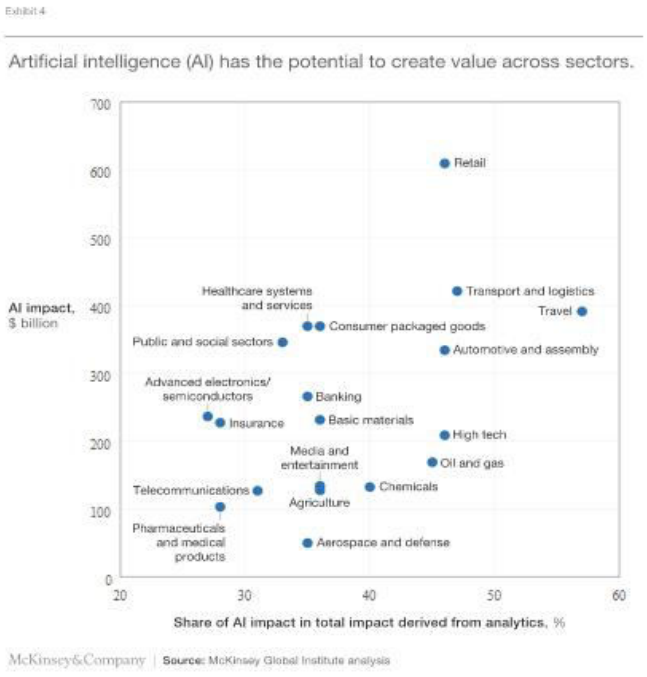

Figure (d). AI Impact derived from analytics.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 8, August 2021 ||

| DOI:10.15680/IJIRSET.2021.1008157 |

Biometric passwords and logins are constantly changed by patients, distributors, and other third parties, which creates a significant gap in the use of Artificial Intelligent tools and procurement stakeholders. Thus, hackers can select pain points thus controlling the employment of information such as ant kills their encouraging growth by revealing their address, bank details, and other personal information. There is little doubt that cybercriminals will continue to access sensitive data in order to discover additional patients or supplier lines.

- According to a CheckPoint study [9], the number of ransomware assaults worldwide is expected to climb to 102 by 2021, with our country having a significant impact on 213 attacks per week. You may probably guess what happened during that assault! Cybercriminals target them by sending malware or other infections to your phones or the mobile networks you're currently using. This infects devices such as mobile phones and laptops connected to it, giving attackers access to all of your sensitive information. No one can now stop those cybercriminals from demanding a ransom (the amount required to release prisoners) and harassing you for it! More than 1000 businesses are affected monthly as a result of this ransomware attack, and the number will grow if businesses do not reinforce their cyber security models or prevent their business aspects from being targeted by criminals.

- On the other side, spear-phishing is a minor component of stealing sensitive information and its very advanced version. Online fraud sends out harmful emails to well-researched victims in this case (such victims are carefully analyzed by cyber attackers for psychological and emotional reasons). [5] According to Verizon's investigative report from 2021, 29 207 real-time security occurrences were investigated, with 5285 of them being confirmed as data breaches. In this example, theft of sensitive information accounts for 36% of the incidents, up 11% from the previous year. When it comes to the spear attack of the crime of stealing sensitive information, the number isn't mentioned, but there is debate of the guaranteed focus. Approximately 95% of enterprises are affected by this type of stolen spear attack and 61% of the data breaches are related.

- When it comes to a tech behemoth or a well-known automation firm, employees are given specific privileges, putting financiers at danger of significant losses. All of this poses a threat from within. In the last two years, they've risen by 47 percent, and they've successfully enticed cybercriminals to properly feed their fraudulent activities.
  According to the Data Breach Report fig (e), these threats affect more than 34% of firms each year, providing a chance for risk breaches to harm customer trust and reputation. Businesses do not take internal threats seriously because they believe it is more necessary to deal with complex market trends than to look at such risks! All of this has thrown the company's current situation into disarray, as their employees have agreed to make deals with hackers in exchange for access to sensitive company information. Later, those thieves gained access to the security systems of the companies on the second list. If enterprises continue to look down on them and delay in restricting their rights, it will be difficult for them to prohibit their employees from engaging in damaging and careless activity in other areas that violate the established cyber security terms.

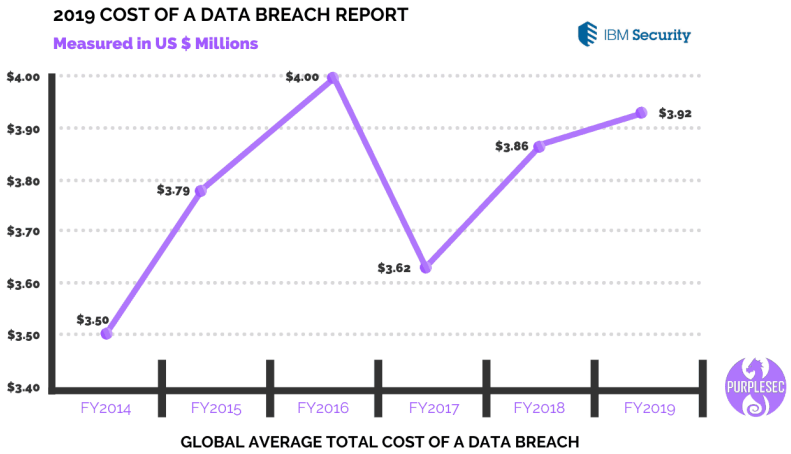

Figure (e). Data Breach report of Small Businesses.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 8, August 2021 ||

| DOI:10.15680/IJIRSET.2021.1008157 |

V. SOLUTIONS

The protection of interconnected systems, including hardware, software, and data, from cyber-attacks, is known as cyber security. Most of today's professionals focus on determining the best way to defend everything from computers and phones to networks and databases from hackers. So the modern cyber security uses various tools, processes, and principles as a solution to protect information.

- **BluVector :**

Real IT technicians and cybersecurity systems seem to be under attack. New attack methodologies, such as malware delivered without attachments, are depleting resources and putting systems to the test.
To begin with, new threats and attack strategies sometimes have a narrow moment of opportunity to penetrate through several defenders before defense catch up.
Second, even if essential threats such as malware are eliminated, defenders due to the constant flood of false positive notifications, the system is likely to be overworked. Tasking machines and computers with self-protection is one approach that has lately become available. It is a security program that could be programmed the thing that acts like an unleashed then it could try and count malware and human back intrusion at machine speed. A move that could give defenders a serious home code advantage this exactly a BluVector defender. BluVector [6] works almost right away that also has deep machine learning capabilities so it is even smarter over the period and to learn each network that deploys its quacking algorithm and detection engines in a way that makes more sense for the sake of the climate. BluVector has either a physical network appliance or a virtual computer deployed. It can operate in sync with network traffic, detecting and removing threats in real time in an effort to keep its space safe that can scan the work perform by other programs and unleash catching threats that might have missed unrecommending fixes. It's built to handle all IPv6 traffic as well as earlier IPv4 streams, allowing it to work in an environment with a lot of IOT control systems and data collecting devices.

- **Bricata:**

An intrusion prevention system or an intrusion detection system is already featured in even the most basic cyber defense measures for any moderate to large corporations. A very well IPS / IDS system that is national surveillance by a security team will identify the bulk of connectivity problems and data leaks by itself. Nevertheless, many corporations have one effective approach specially formulated to handle an IDS blind hole, as evidenced by the fact that many corporations have halted here.
At its highest level, the BRICATA platform [12] remains active. Bricata protects network traffic and key assets with sophisticated IPS/ IDS security that includes various detection engines and threats. This will help the organisation to continue looking for tactical decisions using the same individuals and technologies that they use for IPS inspection. It would be a positive step forward in the quest for greater defense without the ping of loading extra features or retraining staff looking first a Bricata as a pure ideal system, it is installed as a physical or virtual appliance it acts as a the focal point and the module. This intern links up to networks sensors that are installed on a network choke point to capture traffic in data while Bricata sensors are generally often positioned at networking gateways, they may also be positioned around core assets of internal points to provide platform transparency into horizontal changes of future threats when network traffic drops. .Now it takes care of intrusion detection system.

- **Mantix4 :**

Because of the true extent of emerging attacks, any business of the any scale will almost certainly be stolen or penetrated at some point, irrespective about what or how often cyber safety precautions are in existence.
The Mantix4 platform, named after the apex predator of the insect kingdom, the praying mantis, aims to address people's issues while also providing clients with powerful threat hunting capabilities.

Threat hunting is integrated into the Software as a Service by the company, which employs a team of professionals to hunt on their behalf (SaaS). Mantix4 was created for the Canadian government's bureau of community defense, which is analogous to the US Department of Homeland Security. In Canada, Mantix4 helps to protect the system seating in ten sectors, considered critical infrastructure routing out threats that might bypass more traditional protection. This system is deployed as two components, The first part consists of an observer sensor that sits alongside routers or at network gateways at critical points within a protected network, though they can be deployed almost anywhere depending on their needs. The sensors are lightweight and must be contained within the virtual environment or within a

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 8, August 2021 ||

| DOI:10.15680/IJIRSET.2021.1008157 |

data center with special restrictions. The observer sensor, on the other hand, is processed and captures an amount of visitors. the capability will most likely be as a tiny device that just hosts the company's services. The sensors can be set to work inline or depressively sniffed network traffic**.**

- **SecBI :**

This tool [7] covers all the important aspects of any industry level cyber security plan i.e. traffic analysis**.** Network traffic analysis tools have been used for a long time to improve efficiency and corporate network performance by locating underutilized capacity bandwidth and eliminating choke spots. It has lately been utilized as a component of cyber security solutions, which makes sense given that, aside from insider threats, attacks will be initiated, finished, and managed by external parties. The communication between the inside threat virus and its handlers on the outside is recorded using traffic analysis methods. The issue is that the reasoning behind the use of traffic analysis software is incorrect. Although cyber security is strong, the truth is that even a small to medium-sized business will create 3 to 4 billion logs every month. Whether it's human or computer-assisted help, no person will be able to go through it and discover anything useful.Traditionally, capturing all of that data has necessitated the installation of network traps on all network gateways, for an organization with branch offices or remote locations the no of trap installation can be planned pretty high, and even then it's possible that some traffic will get through the gates.
SecBI has been updated with new software aimed at addressing both of these issues: the volume of data required for actionable intelligence threats and the dependency on network traffic technology. They accomplished this by providing their analyzer as a software module that really can perform on premise or in the cloud, and it just looks at log files, so no network traps, client agents, or anything other than access to generate files are required, If finely-tuned Algorithms are used to crunch those billions of events in the logs in search of patterns connected to ongoing attacks or a progressive persistence threat, it can be deployed with as a pay as you go contract where users only pay on basis of how many gigabytes log files data to be process.

VI. CONCLUSION

In the contemporary state of cyberspace, the organization, an individual gets online to survive and set its priorities resources on the webserver that are explicitly available through the HTTP interface. By making all these resources secure the organization must follow certain safety standards or guidelines. Unfortunately, security solutions are mostly static-based signatures if any signature is present detect the malicious activity or vice versa. As a result, a robust solution is required to combat future dangers that arise on a daily basis. Furthermore, there is a semantic requirement for a solution that can comprehend the context of dangers prior to preparation.

VII. ACKNOWLEDGEMENTS

We would prefer to thank Prof. Swapna Augustine Nikale. Department of Information Technology, and B. K. Birla College (Autonomous) Kalyan for providing us with guidance throughout our research work.

REFERENCES

[1] Humayun, M., Niazi, M., Jhanjhi, N. *et al.* Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study. *Arab J SciEng* **45,** 3171–3189 (2020). https://doi.org/10.1007/s13369-019-04319-2
[2] Blog, Josh Fruhlinger, CSO India, "Marriott data breach FAQ: How did it happen and what was the impact?" available at SSRN https://www.csoonline.com/article/3441220/marriott-data-breach-faq-how-did-it-happen-and-what-was-the-impact.html
[3] Crosignani, Matteo and Macchiavelli, Marco and Silva, André F., Pirates without Borders: the Propagation of Cyberattacks through Firms' Supply Chains (May 27, 2021). FRB of New York Staff Report No. 937, Rev. July 2021, Available at SSRN: https://ssrn.com/abstract=3664772 or http://dx.doi.org/10.2139/ssrn.3664772
[4] A. Razzaq, A. Hur, H. F. Ahmad and M. Masood, "Cyber security: Threats, reasons, challenges, methodologies and state of the art solutions for industrial applications," 2013 IEEE Eleventh International Symposium on Autonomous Decentralized Systems (ISADS), 2013, pp. 1-6, doi: 10.1109/ISADS.2013.6513420
[5] Verizon, 2021 Data Breach Investigation Report, available at SSRN https://www.verizon.com/business/en-nl/resources/reports/dbir/
[6] S. Miserendino, C. Maynard and J. Davis, "ThreatVectors: contextual workflows and visualizations for rapid cyber

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 8, August 2021 ||

| DOI:10.15680/IJIRSET.2021.1008157 |

event triage," 2017 International Conference On Cyber Incident Response, Coordination, Containment & Control (Cyber Incident), 2017, pp. 1-8, doi: 10.1109/CYBERINCIDENT.2017.8054637.

[7] Isamu Nakagawa, "SecBI: Cyber Threat Intelligence", available at SSRN https://web.wpi.edu/Pubs/E-project/Available/E-project-032217-152348/unrestricted/SecBI-Cyber-Threat-Intelligence.pdf

[8] Report, Tom Wheelar and David Simpson, "Why 5G requires new approach to cyber security" September 3 2019, available at SSRN https://www.brookings.edu/research/why-5g-requires-new-approaches-to-cybersecurity/

[9] Blog, Check Point Software Technology Ltd, "The New Ransomware Threat: Triple Extortion" available at SSRN https://blog.checkpoint.com/2021/05/12/the-new-ransomware-threat-triple-extortion/

[10] Marlese Lessing, "Case Study: WannaCry Ransomware." 2020 available at SSRN https://www.sdxcentral.com/security/definitions/case-study-wannacry-ransomware/

[11] Blog, John Breeden II , CSO India, " Mantix4 provides threat hunting as a service" in 2018, available at SSRN https://www.csoonline.com/article/3247777/review-mantix4-provides-threat-hunting-as-a-service.html

[12] Blog, Bricata, "his Independent Cybersecurity Product Review Doubles as an Outline for How to Start Threat Hunting with Existing Tools and Skills", available at SSRN https://bricata.com/blog/cybersecurity-product-review-soc/

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.569

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details