Webology (ISSN: 1735-188X)
Volume 18, Number 6, 2021

A Review on NIST, ISO 27001, HIPAA and MITRE ATT&CK Cybersecurity Frameworks

Gurinder Pal Singh[1], Vishal Bharti[2], Manish Kumar Hooda[3]

[1]Research Scholar, Computer Science and Engineering Chandigarh University, Gharauan, Punjab.

[2]Additional Director, Computer Science and Engineering Chandigarh University, Gharauan, Punjab.

[3]Sci/Eng-'SF', Head-Technology Development Division, Semiconductor Laboratory S.A.S.Nagar, Punjab.

Abstract—The aim of this review paper is to discuss Cybersecurity threats, defenses, and some of the security frameworks. Today, the wars between the nations are not on the fields; they are through cyber wars to breach the confidential information of their enemies and use it when required. "Various guidelines and security frameworks have been created to protect the confidentiality, integrity, andavailability of Information systems". Today we face cyber-attacks in every field, whether it's a space (satellite), the air (aviation system), under water (submarines) or on the surface. The world is connected, so it is vulnerable. If you are not connected to any device or network, that means you are safe in today's world. To mitigate the cyber threats or cyber-attacks, many security frameworks have been developed. Acybersecurity framework is a predefined structure that contains the processes, practices, and technologies that enterprises can use to protect their networks and computer systems from security threats. We discussed some of the security frameworks like ISO 27001, NIST, MITRE ATT&CK, HIPAA etc. and their use to counter cyber-attacks.

Keywords—Cyber-attack, Security Framework, MITRE ATT&CK, NIST, ISO 27001

I. INTRODUCTION

The term "Cyber Security" is very well known to everyone. If something goes wrong, I mean if any guidelines are compromised, your valuable data gets hacked or compromised. Zero days' vulnerabilities occur on a daily basis. The rise of cyber-attacks has seen a very sharp increase during the pandemic, because all work started in online mode, but we are not ready for this. As a result, the increase of cyber-attacks has increased. We see the rise in mobile attacks as the use of mobiles increased during the pandemic because the average time spend on smartphones increased by 25%. The impact of COVID-19 on cyber security increases tremendously because the restrictions imposed by government on businesses

force companies to Work from Home (WFH). The company's policies have been changed and somehow compromised, which leads to cyber threat to individuals and organizations.

In its report, Gartner predicts that monetary effect of Cyber Physical Systems (CPS) bringing about lethal setbacks will reach more than $50 billion by 2023 [1]. By 2025, digital assailants will have weaponized Operational Technology conditions to effectively mischief or kill people. Reports of cyber-attacks across India from 2015 to 2020 increased because of compromised security systems. From introduced informational indexes to phishing attempts, malware to outcast data spills, the year 2020 was known as the time of information delicacy. In the primary quarter of 2020, uncovered records were pacing at a development of 273% over a year ago. A client care data set of nearly 280 million client records from Microsoft was exposed on the dark web for sale [2]. The MGM Resort database exposed over 10.6 million hotel guests in February, 2020. The E-mail, password, personal meeting URLs and hostkeys of over 500,000 Zoom teleconferencing coordinating records were found on sale on the dark net at the prize of $.02. Beside this, many other world-renowned companies like BlueLeaks, Cognizant, Twitter,Instagram, TikTok & YouTube, etc. lost their data. With 3950 confirmed data breaches in 2020 [3], The year 2020 broke all records when it came to the loss of data breaches and cyber-attacks. More than 1.1 million cyber-attack were reported across India in 2020. This was a significant increase during the COVID-19 pandemic as compared to the previous year. There were 137.7 million new malware tests in 2020 and we are presently at 92.45 million new examples in 2021 [4].

The following graph shows the most recent 10 years of expansion in malware that the AV-TEST Institute enrolled more than 450,000 new malevolent projects (malware) and possibly undesirable applications (PUA) [5].

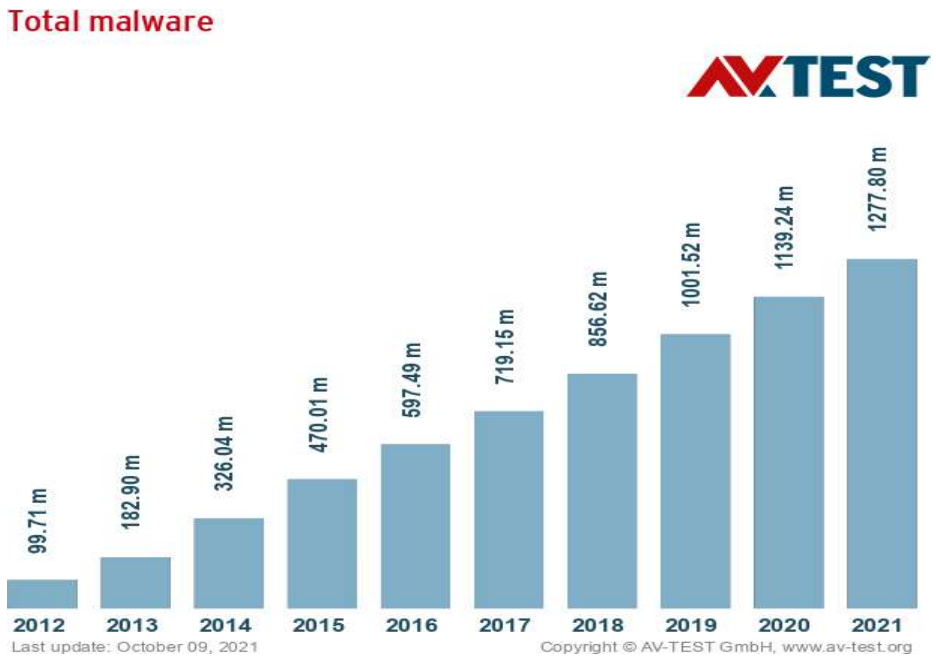

Fig. 1. 10 year increase in malware [6]

WFH culture compromise the security. The impact of cyber threats is so high that, as per CERT-In, there are 300% increase in cyber threats. The three standards of Information Security - Confidentiality,

Integrity and Availability – otherwise called CIA triad - were compromised. The reason behind this is a lack of information regarding cyber security and work pressure.

II. CYBER SECURITY FRAMEWORKS

Security experts, with the help of governments, develop cybersecurity frameworks that provide a common set of standards and rules for security. These rules are framed to counter cyber threats and secure organizations and industries. With the help of cybersecurity framework, it becomes easier to understand the attack pattern of the threat actor. The idea is to stop the attacks before they happen. With the help of cybersecurity frameworks, organizations can easily define the processes and procedures to access,monitor, and mitigate cybersecurity threats. To secure all the vulnerabilities, the following cybersecurity frameworks are used:

A. NIST Cybersecurity framework

The National Institute of Standards and Technology (NIST) was established in response to the executive order of the then American president, Obama. The framework was established to protect critical infrastructure from cyber-attacks. The NIST framework supplements and does not supplant associations hazard boards interaction and network protection program. The first version of NIST cybersecurity Framework was released on February 12, 2014. By 2015, more than 30% American organizations have started implementing it. Gartner estimated that it would be adopted by 50% of American organizations by the year 2020 [7].

The NIST framework is a danger-based approach to overseeing network protection hazard and composed of 3 parts or components:

i. The Framework Core

ii. Framework Implementation Tiers.

iii. Framework Profiles.

The framework core consists of 4 elements and 5 concurrent and continuous functions:

TABLE I. THE FRAMEWORK CORE

The Framework Core	
Elements	**Functions**
Functions	Identify
Categories	Protect
Sub-Categories	Detect
Informative References	Respond
	Recover

The structure execution levels portray an association that rehearses over a broad reach from, Partial (Tier 1) to Adaptive (Tier 4). During the level decision collaboration, an affiliation should consider its current risk, the executive's practices, danger environment, legitimate and regulatory necessities,

business/mission targets, and definitive prerequisites. The NIST Cyber Security framework has 5 Functions, 23 Categories, 108 Sub-Categories and 6 Informative References. Structure Profiles address the results depending on the business needs that an association has chosen from the system classes and sub-classifications. Organizations can develop its own profiles. To develop a profile, an organization can review all the categories and sub-categories based on its own mission and risk assessment.

B. ISO 27001 and ISO 27002

The International Organization for Standardization (ISO) is an association established 1946 and upheld by 159 nations [8]. ISO is the main giving body for International Standards. The ISO 27001 was distributed in 2005 under the title "Information Technology-Security Techniques-Information Security Management Systems-Requirements" [8]. The ISO 27001 and ISO 27002 confirmations are viewed as the global norms for approving a network safety program inside and across outsiders [9]. ISO 27001 isan International Standard in Information Security and Management Systems and this assists with guarding purchaser information in government offices and in the private area [10]. An organization having ISO affirmations can exhibit to the board, clients and partners that they are cyber security agreeable and have executed online protection strategies.

The ISO 27001 can be executed in an association, benefit or non-benefit, private or public, little or huge. There are four fundamental business helps that an organization can accomplish with the execution of this data security standard:

1. Achieve marketing advantages.
2. Comply with legal requirements.
3. Lower costs.
4. Better organization.

The ISO 27002 standard showed how a security cosmology can be utilized to expand the proficiency of the consistence actually looking at process [11]. The ISO 27002 standard says that there should be an information reinforcement methodology set up in the event of information theft. The security of a customer's data is important and should be in place.

C. HIPAA

The health Insurance Portability and Accountability Act (HIPAA) is a network safety system that requires medical services associations to execute controls for getting and securing the protection of electronic wellbeing data [9]. HIPAA is such a powerful act that it is known as total silence all the time [12]. Hospital waiting rooms are public places, so you cannot announce the name of a patient aloud. Only communication by hand signals are allowed. Indeed, even telephone system has been recognized asa dangerous type of correspondence by HIPAA controllers.

HIPAA regulates US Protected Health Information (PHI) usage and disclosure. HIPAA alludes just to a sub-arrangements of associations medical care plans and medical care installment frameworks [13]. Collecting and using health care data for research is also controlled by HIPAA. HIPAA comes with 11 rules, and all these 11 rules make sure that policies and procedures are in place for the privacy protection

of patients. A Patient's record should be kept safe for six years. Six of the 11 principles of HIPAA have been delivered for execution [14]:

- Transactions and Code Sets
- Privacy
- Standard Unique Employer Identifier
- Security
- Enforcement
- Standard Unique Healthcare Provider Identifier Rule.

D. MITRE ATT&CK

MITRE is a Corporation that developed the Attack Tactics & Techniques, for Common Knowledge (ATT&CK) Framework. It was founded in 2013 as government funded cybersecurity research and development organization based in the United States. ATT&CK is an open system and information based of enemy strategies and methods dependent on genuine perceptions [15]. This framework helps usto identify real threats and classify them into various categories. With the help of attack tactics and techniques, we can identify certain types of attack behaviors. ATT&CK framework uses four use cases:

1. Threat Intelligence
2. Detection & Analytics
3. Adversary Emulation & Read Teaming
4. Assessments & Engineering

ATT&CK is a knowledge base of adversary behaviors. It is like an encyclopedia of different activities by cyber criminals. The best thing about MITRE ATT&CK is that it is free, open and globally accessible. It is contributed by the community, based on real-world observations and shares a common language ATT&CK helps us to understand how an adversary operates and helps detect or stop these behaviors using analytics, hence preparing the organization from an adversary trying to harm them. It helps the Blue Team to stop the adversary there and then when they notice the flagged behaviors.

The term "Kill Chain" is a military concept and it is used to describe the structure of an attack. In 2011, Lockheed Martin computer scientist pioneered the concept of Cyber Kill Chain in Information Security [16]. The military kill chain model is "F2T2EA", which is: Find-recognize the objective, Fix- fix the Objective, Track-screen the objective development, Target-select a suitable weapon, Engage- Apply the weapon to the objective, Access-Evaluate impacts of the objective.

Using this attack model, Lockheed Martin introduced a new "Intrusion Kill Chain" model to define computer security network in 2011 [16]. According to Lockheed Martin, a threat must progress through the seven phases. They are Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command & Control, and Actions on Objectives. These 7 phases are mentioned in fig 2.

Fig. 2. 7 Phases of Intrusion Kill Chain [16]

There are two fundamental differentiations between MITRE ATT&CK and Cyber Kill Chain:

1. The MITRE ATT&CK structure digs further into how each stage is directed by ATT&CK strategies and sub-procedures. The framework is regularly to keep track the assault plans.
2. The Cyber Kill Chain doesn't factor in the different strategies and procedures. The Cyber Kill Chain structure expect that an enemy will pass on a payload, for instance, malware to the objective environment.

The MITRE ATT&CK as on date, has three iterations:

1. ATT&CK for Enterprise: It centers around antagonistic conduct in Windows, Mac, Linux, and Cloud environments.
2. ATT&CK for Mobiles: It centers around antagonistic conduct on iOS and Android working framework.
3. Pre-ATT&CK: It centers around "pre-taking advantage of" ill-disposed conduct. Pre-ATT&CK is incorporated as a component of the ATT&CK for Enterprise matrix.

The MITRE ATT&CK framework is comprise of Tactics, Techniques and Procedures (TTPs). The highest level of organization in ATT&CK is Tactics [17]. Most attackers gain access through a sequenceof attack Tactics starting from Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, Exfiltration, Command andControl, Impact [17]. Tactics portray what the assailant is attempting to do at some random period of assault, not how they are explicitly going with regards to it.

The conduct model introduced by ATT&CK contains the accompanying two core components:

1. Tactics: Signifying present moment, strategic enemy objectives during an attack.
2. Techniques: Depicting the means by which enemies achieve strategic goals.

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command And Control
10 items	31 items	56 items	28 items	59 items	20 items	19 items	17 items	13 items	9 items	21 items
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Command-Line Interface	AppCert DLLs	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Control Panel Items	AppInit DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery	Exploitation of Remote Services	Data from Information Repositories	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Application Shimming	Clear Command History	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Local System	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Execution through API	Authentication Package	Bypass User Account Control	CMSTP	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Network Shared Drive	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing via Service	Execution through Module Load	BITS Jobs	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Password Policy Discovery	Pass the Ticket	Data from Removable Media	Exfiltration Over Other Network Medium	Data Obfuscation
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Dylib Hijacking	Component Firmware	Forced Authentication	Peripheral Device Discovery	Remote Desktop Protocol	Data Staged	Exfiltration Over Physical Medium	Domain Fronting
Trusted Relationship	Graphical User Interface	Browser Extensions	Exploitation for Privilege Escalation	Component Object Model Hijacking	Hooking	Permission Groups Discovery	Remote File Copy	Email Collection	Scheduled Transfer	Fallback Channels
Valid Accounts	InstallUtil	Change Default File Association	Extra Window Memory Injection	Control Panel Items	Input Capture	Process Discovery	Remote Services	Input Capture		Multi-hop Proxy
	Launchctl	Component Firmware	File System Permissions Weakness	DCShadow	Input Prompt	Query Registry	Replication Through Removable Media	Man in the Browser		Multi-Stage Channels
	Local Job Scheduling	Component Object Model Hijacking	Hooking	Deobfuscate/Decode Files or Information	Kerberoasting	Remote System Discovery	Shared Webroot	Screen Capture		Multiband Communication
	LSASS Driver	Create Account	Image File Execution Options Injection	Disabling Security Tools	Keychain	Security Software Discovery	SSH Hijacking	Video Capture		Multilayer Encryption
	Mshta	DLL Search Order Hijacking	Launch Daemon	DLL Search Order Hijacking	LLMNR/NBT-NS Poisoning	System Information Discovery	Taint Shared Content			Port Knocking
	PowerShell	Dylib Hijacking	New Service	DLL Side-Loading	Network Sniffing	System Network Configuration Discovery	Third-party Software			Remote Access Tools
	Regsvcs/Regasm	External Remote Services	Path Interception	Exploitation for Defense Evasion	Password Filter DLL	System Network Connections Discovery	Windows Admin Shares			Remote File Copy
	Regsvr32	File System Permissions Weakness	Plist Modification	Extra Window Memory Injection	Private Keys	System Owner/User Discovery	Windows Remote Management			Standard Application Layer Protocol
	Rundll32	Hidden Files and Directories	Port Monitors	File Deletion	Replication Through Removable Media	System Service Discovery				Standard Cryptographic Protocol
	Scheduled Task	Hooking	Process Injection	File System Logical Offsets	Securityd Memory					Standard Non-Application Layer Protocol
	Scripting	Hypervisor	Scheduled Task	Gatekeeper Bypass	Two-Factor Authentication Interception					Uncommonly Used Port
	Service Execution	Image File Execution Options Injection	Service Registry Permissions Weakness	Hidden Files and Directories						Web Service
	Signed Binary Proxy Execution	Kernel Modules and Extensions	Setuid and Setgid	Hidden Users						
	Signed Script Proxy Execution	Launch Agent		Hidden Window						
	Source			HISTCONTROL						
	Space after Filename			Image File Execution Options Injection						

Fig. 3 MITRE ATT&CK Tactics [18]

The ATT&CK matrix captures relationships between tactics, techniques, and sub-techniques. ATT&CK is a collection of series and focuses on a specific technology domain or platform and the advisories associated with it. The fig.3 displays the most popular matrix in the Enterprise technology domain. The enterprise domain operates on various operating Systems and specific applications like Windows, Linux, Mac OS, Cloud and Networks. Adversaries target many different technology domains, not just enterprise. In mobile ATT&CK, such as IOS and Android, as well as ATT&CK for Industrial Control Systems. ATT&CK matrices are unique, but often overlap in many ways.

III. LITERATURE REVIEW

We elaborate some of the popular cyber security frameworks and goes through it viz. its types, functions, characteristics, etc.

In his paper titled "Real Time Multi-Stage Attack Detection", Yuvraj Sanjayrao Takey et. al. uses MITRE ATT&CK framework and Machine Learning (ML) for early detection of multi-stage attack in real time [19]. Cert-In labelled dataset is used in their research to train the model. Because selection of ML algorithms is manual and it consumes much time.

Anna Georiadou et. al. developed a Cyber Security Culture Framework using MITRE ATT&CK framework. The author combines organizational and Individual factors to form the Culture framework in a scientific approach [20]. By exploiting ATT&CK database this framework classifies and analyzing the possible security gaps. In this study, the author developed a tool to access the MITER ATT&CK implementation for enterprise and ICS threat lists**.** To deal with the thoughts and behaviors of others, this cultural framework is aimed at both organizations and individuals.

Seungoh Choi et. al. used MITRE ATT&CK to automate the generation of various attack sequences and present application methods through case studies [21]. Industrial Control System (ICS) dataset used in attack sequence to automatically control attack sequences. Hidden Markov Model (HMM) parameters are used for case analysis and its ATT&CK is used to create a realistic attack sequence for the control system. The proposed method cannot be modeled accurately and the model requires manual intervention, which leads to a lack of accuracy and is time consuming.

Legoy et. al. uses the MITRE ATT&CK system to automatically catch the Tactics, Techniques and Procedures (TTPs) utilized by danger actors [22]. To support the community, the author has developed a tool called re ATT that produces automated analysis reports. It uses a multilevel classification technique to automate the extraction of Cyber Threat Intelligence (CTI) information (TTP) from textual cybersecurity reports. This device computerizes intelligible information and concentrate ATT&CK strategies and procedures.

Elitzur et. al. use Cyber Threat Intelligence (CTI) to make hypothesis about attacks. The proposed algorithm provides an Attack Hypothesis Generator (AHG). It consists of unmonitored attack patterns and the tools used by threat actors. AHG proposes new way to reconstruct attack pattern and protect your network. The author used the MITRE ATT&CK framework to improve the accuracy of AHG. The machine learning approach is used to train the model with this large amount of data needed to make a hypothesis.

IV. Conclusion and Future Prespective

While reviewing the different papers, we understand that the MITRE ATT&CK system is utilized to create mechanized digital threat reports, prepare hypothesis to know the threat actor's behavior and the steps of attack, predict the attack sequence, etc. The authors use a machine learning approach for supervised and unsupervised link prediction to train dataset. Takey et. al. used labelled data provided by Cert-In to detect an attack early before it happens, but using machine learning algorithms, the process is slow and time-consuming. Legoy et. al. developed a tool named re ATT to generate automated threat reports with the help of MITRE ATT&CK framework.

Machine learning algorithms usually take a long time to learn about large threats and datasets. With the MITRE ATT&CK framework and deep learning models, cyber-attacks can be thwarted in real time. From an efficiency standpoint, it is possible to compare and analyze datasets and the ATT&CK framework.

References

[1] "Gartner Predicts 75% of CEOs Will be Personally Liable for Cyber-Physical Security Incidents by 2024," Gartner. https://www.gartner.com/en/newsroom/press-releases/2020-09-01-gartner-predicts-75--of-ceos-will-be-personally-liabl (accessed Oct. 09, 2021).

[2] D. Winder, "Microsoft Security Shocker As 250 Million Customer Records Exposed Online," Forbes.https://www.forbes.com/sites/daveywinder/2020/01/22/microsoft-security-shocker-as-250-million-customer-records-exposed-online/ (accessed Oct. 09, 2021).

[3] "2020 Data Breaches - The Most Significant Breaches of the Year | Identity Force®," We Aren't Just Protecting You From Identity Theft. We Protect Who You Are., Jan. 03, 2020. https://www.identityforce.com/blog/2020-data-breaches (accessed Oct. 09, 2021).

[4] "300+ Terrifying Cybercrime & Cybersecurity Statistics (2021)," Comparitech. https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/ (accessed Oct. 09, 2021).
[5] "Malware Statistics & Trends Report | AV-TEST." https://www.av- test.org/en/statistics/malware/ (accessed Oct. 09, 2021).
[6] "print_total_distribution_10-years_en.png (1210×1087)." https://www.av-test.org/typo3temp/avtestreports/print_total_distribution_10-years_en.png?1633796707 (accessed Oct. 09, 2021).
[7] "cockcroft2020.pdf."
[8] "Disterer - 2013 - ISOIEC 27000, 27001 and 27002 for Information Sec.pdf."
[9] E. Cisternelli, "7 Cybersecurity Frameworks To Reduce Cyber Risk," Bit Sight. https://www.bitsight.com/blog/7-cybersecurity-frameworks-to-reduce-cyber-risk (accessed Oct. 10, 2021).
[10] "Faruq et al. - 2020 - Integration of ITIL V3, ISO 20000 & ISO 270012013.pdf."
[11] "Fenz et al. - 2016 - Mapping information security standard ISO 27002 to.pdf."
[12] "See - 2003 - The American Society for HIPAA compliance present.pdf."
[13] "Shuaib et al. - 2021 - Compliance with HIPAA and GDPR in blockchain-based.pdf."
[14] "Kiel - 2010 - HIPAA SOP HIPAA as Standard Operating Procedures.pdf."
[15] "MITRE ATTCK by Randy Franklin Smith, Brian Coulson, Dan Kaiser (z-lib.org).pdf."
[16] "Kill chain," Wikipedia. Sep. 15, 2021. Accessed: Oct. 23, 2021. [Online]. Available: https://en.wikipedia.org/w/index.php?title=Kill_chain&oldid=1044537716
[17] "MITRE ATTCK by Randy Franklin Smith, Brian Coulson, Dan Kaiser (z-lib.org).pdf."
[18] "Snapshot." Accessed: Oct. 26, 2021. [Online]. Available: https://www.rapid7.com/fundamentals/mitre-attack/
[19] Y. S. Takey, S. G. Tatikayala, S. S. Samavedam, P. R. Lakshmi Eswari, and M. U. Patil, "Real Time early Multi Stage Attack Detection," in 2021 7th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, Mar. 2021, pp. 283–290. doi: 10.1109/ICACCS51430.2021.9441956.
[20] A. Georgiadou, S. Mouzakitis, and D. Askounis, "Assessing MITRE ATT&CK Risk Using a Cyber-Security Culture Framework," Sensors, vol. 21, no. 9, p. 3267, May 2021, doi: 10.3390/s21093267.
[21] S. Choi, J.-H. Yun, and B.-G. Min, "Probabilistic Attack Sequence Generation and Execution Based on MITRE ATT&CK for ICS Datasets," in Cyber Security Experimentation and Test Workshop, Virtual CA USA, Aug. 2021, pp. 41–48. doi: 10.1145/3474718.3474722.
[22] "Legoy et al. - Automated Retrieval of ATT&CK Tactics and Techniqu.pdf."