International Journal of Advanced Trends in Engineering and Technology (IJATET)
Impact Factor: 5.965, ISSN (Online): 2456 - 4664
(www.dvpublication.com) Volume 7, Issue 2, 2022

PROACTIVE COMPLIANCE TESTING USING CYBERSECURITY DIGITAL TWINS

Aravind Kumar Karpoorapu
AI/ML Research Specialist, 2100 Legacy Dr Apt 1406, Plano, TX 75023,
United States of America

Cite This Article: Aravind Kumar Karpoorapu, "Proactive Compliance Testing Using Cybersecurity Digital Twins", International Journal of Advanced Trends in Engineering and Technology, Volume 7, Issue 2, Page Number 78-81, 2022.

Abstract:

Proactive compliance testing can use cybersecurity digital twins to test how an organization is performing with respect to selected regulatory and security programs. Virtualization provides an opportunity to minimize risks, allocate resources more efficiently, and meet legal requirements through constructing virtual models of IT frameworks. This innovative technique makes it possible to respond to new risks before they are incurred and strengthen cybersecurity against new threats. Keywords: Preventive measures, IT security, virtual models, legal requirements, attack replicas.

Introduction:

The issue is especially pressing with the growing focus on developing digital tools and services as many organizations struggle to adapt to the plethora of cybersecurity regulations currently in force. Cybersecurity Digital twins are a relatively new approach to protecting organizations: they are mirrored digital copies of the organization's physical IT space. Such digital twins mimic the physical environment where an organization operates, allowing them to evaluate its compliance strategy against such conditions as an attack, an audit by a regulatory agency, or changes to physical infrastructure. Hence, by creating virtual model scenarios to enact policy infractions and testing reactions in parallel, they made an innovative way of monitoring and ensuring the GDPR, the HIPAA-compliant policy, and the ISO 27001 standard. This makes risks reduced, security investments enhanced, and creates trust with the various parties concerned.

Simulation Report:

An exercise, based on a digital twin application, identified key gaps in an organization's readiness for compliance issues. For example, in a specific financial services organization, some results of the DT approach were in the simulation of compliance with the ISO 27001 access control standards. The simulation highlighted a gap in the processes of handling employee credentials with weak passwords and no two-factor authentication in particular. A fake phishing exercise showed just how many people could be entrapped by a simple email scam, proving the importance of the training of the workforce and improvement of the corresponding filter mechanisms.

Furthermore, the simulation assessed the encryption procedures to assess compliance with GDPR. Already, it exposed that many Customer records held in outdated databases are not adequately encrypted. This led the organization to adopt better forms of encryption practices and applicable controls to avert the risks. It is important to realize that these suggestions illustrate the efficacy of using a digital twin to prevent and mitigate compliance issues on the horizon.

Real-Time Scenarios:

Some examples of the usage of cybersecurity digital twins are observed in the cases where compliance testing in advance is rather important. For instance, in a financial institution, a digital twin was used to simulate various cases of unauthorized access to client information. The findings showed insufficient password' policies and the absence of multi-factor authentication. Therefore, the approaches to institution authentication was tightened, the compliance with ISO 27001 standards was improved along with the protection of the records from unauthorized access (Rife, 2019).

HIPAA regulations were assessed using digital twins in a context where a healthcare organization was being tested. In the simulation, it was realized that weak and outdated firewall settings were among the main issues depriving the network of the ability to resist an intrusion. This led the organization to improve their firewall infrastructure and add more comprehensive intrusion detection system (IDS); thus, meet compliance and enhance security (Gepp et al., 2018).

In the technology sector, one company used their digital twin to audit the company's cloud for ISO 27001 compliance. The simulation pointed at unencrypted storage buckets in Amazon as a compliance issue. This made the organization enhance encryption and analyze its data access policies. Besides, compliance was achieved, and the security of its cloud-based operations was improved as well (Di Dario et al., 2018).

Table 1: Impact of Multi-Factor Authentication (MFA) Implementation

Time Period	Unauthorized Access Attempts (Before MFA)	Unauthorized Access Attempts (After MFA)
Week 1	50	20
Week 2	60	15
Week 3	45	12
Week 4	55	8

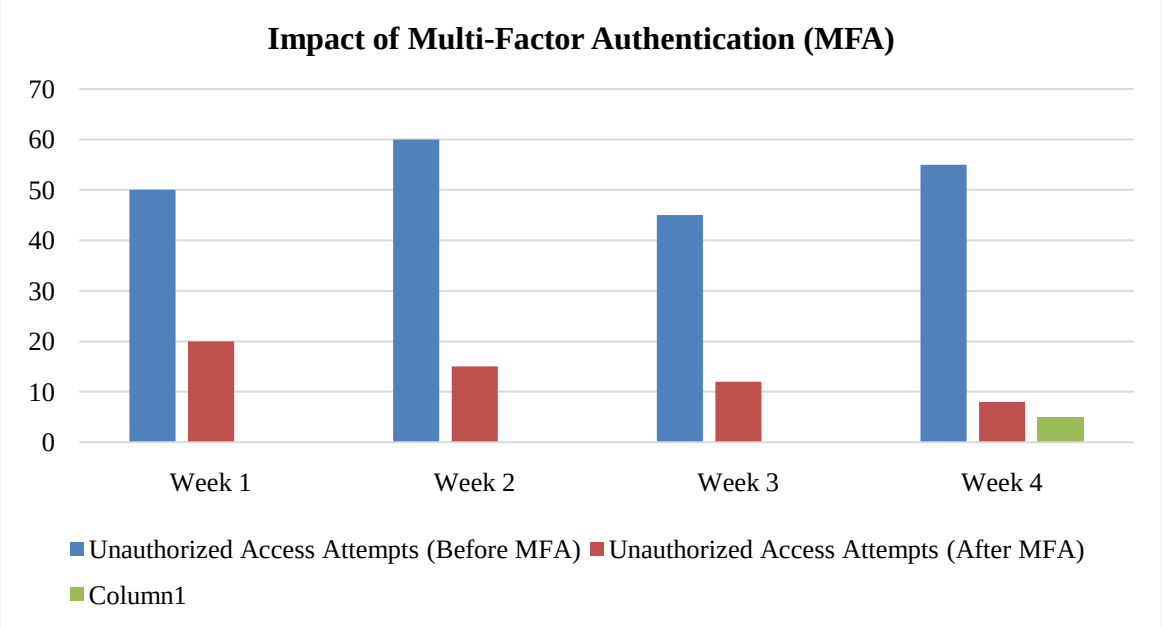


Table 2: Firewall Configuration Impact on Intrusion Detection

Month	Intrusion Attempts Detected (Before Upgrade)	Intrusion Attempts Detected (After Upgrade)
January	100	20
February	120	18
March	95	15
April	110	10

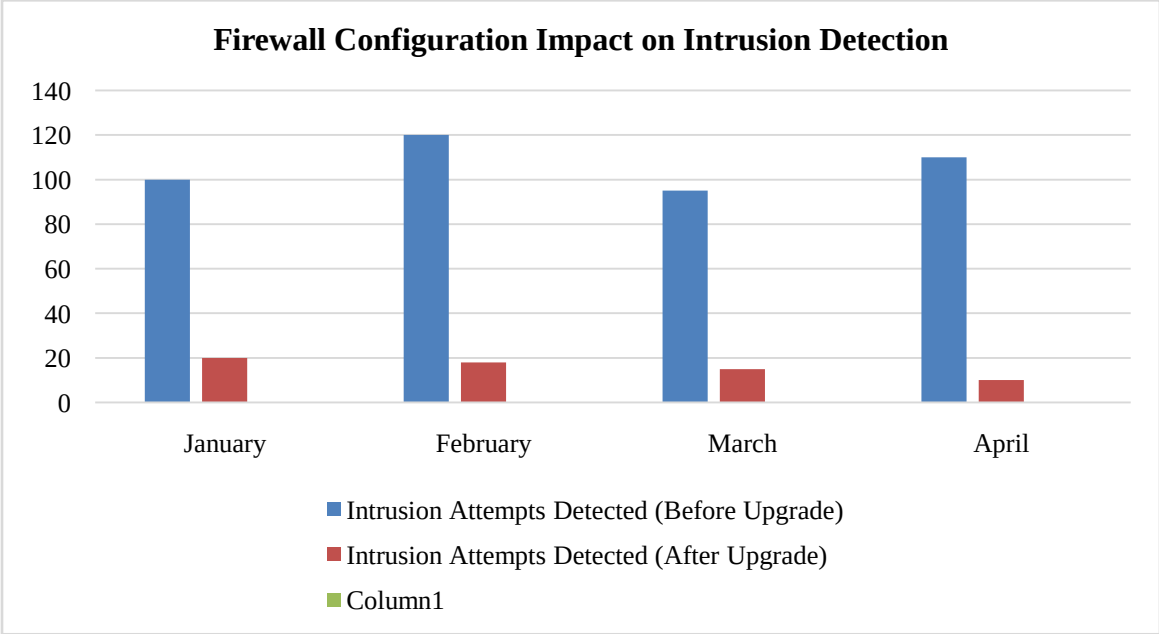
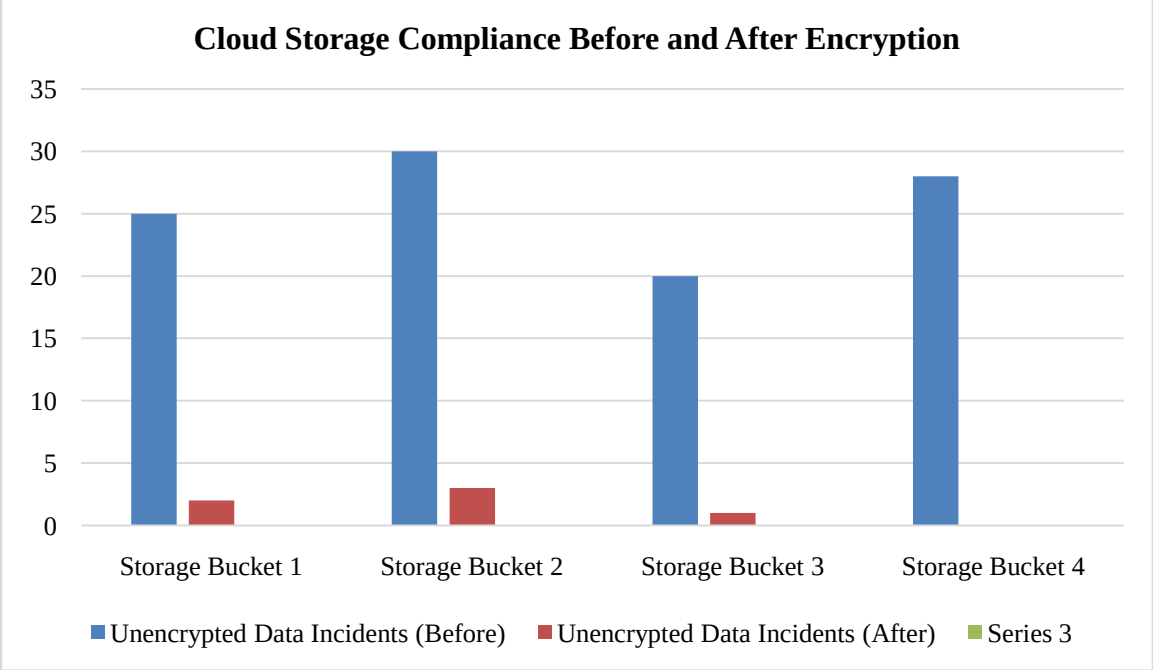


Table 3: Cloud Storage Compliance Before and After Encryption

Category	Unencrypted Data Incidents (Before)	Unencrypted Data Incidents (After)
Storage Bucket 1	25	2
Storage Bucket 2	30	3
Storage Bucket 3	20	1
Storage Bucket 4	28	0



Challenges and Solutions:

Another problem of applying cybersecurity digital twins is that their incorporation into legacy structures is quite complicated. Different complexities exist in implementation since older systems may not be interoperable with the digital twin technologies of the present age, thus requiring radical procedures such as redesigning. This problem can be solved by adopting phased digital twin implementation strategies that allow the organization to extend digital twin use over time while keeping the operations going (Stoddart, 2016).

The second big issue is related to data protection issues. Games that replicate actual organizational environments require manipulation of organizational information, which may not be well protected against exposure in the course of the game. To address this risk, management should use the highest level of encryption and develop safe simulation spaces. This enables the different levels of tests to be carried out with the utmost confidentiality of the information that is being processed (Laamarti, 2019).

The high cost of creating as well as maintaining the digital twin is another issue that is invocable. This means that some of the hardware, software and expertise essential to effective record keeping can be beyond the reach of some organizations due to their size. Industry consortiums or partnership can come in handy for spreading costs and resources required in coming up with the digital twin technology (Fernandez-Carames & Fraga-Lamas, 2019).

Conclusion:

Cybersecurity digital twin-performed proactive compliance testing is the breakthrough to protect organizational infrastructure and meet the legal requirements. Through the creation of realistic threats and dealing with threats before they emerge as adversities, organizations can increase their strengths of cybersecurity defense and compliance compliance measures. Such innovative strategy does not only manage the risks but also builds up credibility and robustness in the more digitalized and regulated environment of today.

References:

1. Fernandez-Carames, T. M., & Fraga-Lamas, P. (2019). A review on the application of blockchain to the next generation of cybersecure industry 4.0 smart factories. IEEE Access, 7, 45201-45218. https://ieeexplore.ieee.org/abstract/document/8678753/

2. Gepp, A., Linnenluecke, M. K., O'Neill, T. J., & Smith, T. (2018). Big data techniques in auditing research and practice: Current trends and future opportunities. Journal of Accounting Literature, 40(1), 102-115. https://www.emerald.com/insight/content/doi/10.1016/j.acclit.2017.05.003/full/html
3. Laamarti, F. (2019). Towards Standardized Digital Twins for Health, Sport, and Well-being (Doctoral dissertation, Université d'Ottawa/University of Ottawa). https://ruor.uottawa.ca/handle/10393/39502
4. Ngadi, M. A., & Gungor, V. C. (2018). Computer Science Review. https://www.academia.edu/download/114179351/j.cosrev.2018.08.00120240505-1-qmuj5.pdf
5. Rife, R. H. B. H. (2019). Improving Information Security Awareness Training through Real-Time Simulation Augmentation (Doctoral dissertation, Northcentral University). https://search.proquest.com/openview/f50c6f f238c7b134b8b4be517ca02b
6. Stoddart, K. (2016). Live free or die hard: US-UK cybersecurity policies. Political Science Quarterly, 131(4), 803-842. https://academic.oup.com/psq/article-abstract/131/4/803/6846413