Using Threat Intelligence to Assess the Effectiveness of Cybersecurity Controls

Confidentiality Notice

Abstract

This document presents an analysis of cyber-attack techniques observed from 2019 to 2023. The study employed the MITRE ATT&CK framework to identify and categorize 194 unique attack techniques, tallying a total of 20,812 observations across the period. Key findings highlight the evolving nature of cyber threats and the effectiveness of minimum controls implemented by cyber insurers to mitigate these risks. The analysis reveals a significant decline in the protection level of these controls over time, suggesting that attackers are developing methods to circumvent them. The report recommends adopting intelligence-led and tailored guidance for cybersecurity practices to enhance the robustness of defenses against sophisticated and evolving threats.

Method

Data Collection

Collection Sources

Canopius' Threat Intelligence repository is built upon various data sources, including:

- Data collected by our Cyber Incident Management Team
- Insights, Threat Reports, and Threat Feeds from Panel Vendors
- Loss Data from Claims
- Open Source Intelligence, News, and Forums (collected using *Eclectic IQ*)
- Premium Threat Intelligence Partnerships (*Group-IB*)
- Outside-In Scanning tooling (*BitSight Technologies*)

Each of the above data sources were used in this analysis.

Data Set

We were interested in identifying all the *Attack Techniques*, and the number of observations, from the above data sources.

Attack Techniques are individual actions that a threat actor makes as part of an attack to realize their goal. An individual attack or incident may comprise of multiple *Attack Techniques*.

From the above data sources, we gathered a list of all the attack techniques observed across incidents, attacks and claims. We used the *MITRE ATT&CK* framework to differentiate and identify attack patterns/techniques.

We collected techniques for the last 5 complete calendar years: 2019 through to 2023.

Overall, our data set included 20,812 techniques identified across all attacks, which covered 194 unique techniques types. **Table 1** details the number of techniques observed across each calendar year.

Year	Number of Observed Techniques	Number of Unique Techniques
2019	2993	192
2020	3709	187
2021	3826	187
2022	5873	192
2023	4411	191

Table 1: Observed and Unique Techniques collected across each Calendar Year

Mapping Techniques to Controls

We investigated the following controls, given these are the standard 'minimum controls' implemented by cyber insurers:

- Backups & Secure Backup Storage
- Email Security Filtering
- Endpoint Detection & Response
- Multi-Factor Authentication (MFA) for Remote Access
- Privileged Account Management
- Security Awareness Training

Our Minimum Controls were mapped to each observed technique. A 'mapped connection' was made if the minimum control was known to protect against the attack technique.

Calculating a 'Protection Level'

For each year, and for each control, we calculated a *Protection Level.*

The *Protection Level* of a control is the proportion of observed attack techniques within a data set that were mitigated against by the control.

Results

The results in **Table 2** list the calculated protection levels for each control.

Year	Protection Levels						
	MFA	PAM	Backups	Training	Email Security Filtering	EDR	Combined (Stacked)
2019	4%	34%	0.4%	22%	9%	28%	96%
2020	9%	36%	3%	9%	0.2%	17%	76%
2021	14%	33%	3%	13%	0.3%	10%	74%
2022	4%	35%	0.3%	5%	0.5%	21%	66%
2023	9%	18%	0.4%	8%	0.2%	13%	48%

Table 2: Protection Levels of Minimum Controls from 2019 through to 2023

The *Combined (Stacked)* protection level is the sum of the protections levels but does not adjust the combined protection level for techniques that are protected by *multiple* controls, otherwise known as overlapping protection.

The results from **Table 2** are visualized within **Figure 1** below.

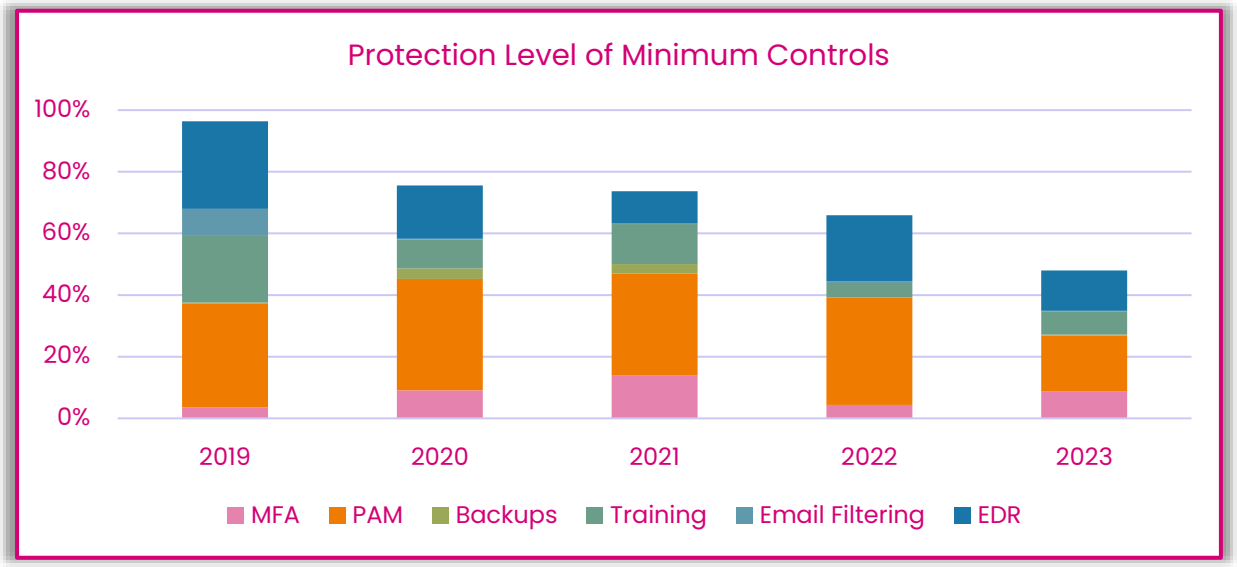

Figure 1: Protection Levels of Minimum Controls from 2019 through to 2023

In **Figure 1** we can see that the combined (stacked) protection level of all the minimum controls is near 100% in 2019 – before minimum controls were implemented by insurers.

Minimum Controls start being enforced by insurers in 2020/2021. After this, we begin to see a decrease in combined protection level of the minimum controls. In 2023, the minimum controls had a combined protection of 48%, combined to 96% in 2023.

Conclusion

The steep decrease in protection offered by the minimum controls demonstrates the volatility of the cyber threat landscape.

The trends observed in **Figure 1** demonstrate that attackers are diversifying their attack techniques in order to bypass the controls that are becoming more commonplace. This may be, in part, due to minimum requirements from cyber insurers driving up the baseline of security standards.

We have 2 key takeaways from the above analysis:

1. Intelligence-Led Guidance & Advice

Given the volatility of the cyber threat landscape, it is important that organizations, and their advisory partners (including insurers) stay on-top of the cyber threat landscape and ensure that the "best practices" are up-to-date and informed by the latest attack patterns and threats. Threat Intelligence plays a pivotal role in determining best practice guidance.

Using this same analysis approach, we can use threat intelligence to identify what the controls are that "plug the gap" in the protection level.

2. Tailored Guidance

As we improve security baselines across the board, attackers will develop new methods of bypassing the newly implemented security mechanisms. As insurers, we have a strong influence on security baselines by recommending minimum standards that are then implemented across the industry. Unfortunately, these minimum standards are becoming easy to predict, which is contributing towards the decline in protection level of minimum controls.

We should move away from a "one-size-fits-all" approach to minimum standards. Security control guidance should be tailored towards an individual insured, based on their unique firmographic characteristics and corresponding threat profile. Custom and prescriptive standards result in a greater level of protection, as well as a security stack that is harder for a threat actor to predict.