Cybersecurity Theater

White Paper

Crytica Security
7655 Town Square Way
Suite 212
Reno, NV 89523

Website: CryticaSecurity.com
Email: info@cryticasecurity.com

Cybersecurity Theater

Contents

1. INTRODUCTION – REPEATING HISTORY WITH SECURITY THEATER

If you want peace, prepare for war[1]

George Santayana's oft-quoted observation that "Those who cannot remember the past are condemned to repeat it."[2] is as relevant today as when he wrote it. For all of this insight's countless citations and repetitions, it appears that the only thing we ever learn from the past is that we never learn from the past. Somehow, the present always seems to be just a little bit different, and the past just a little bit less relevant. The technology is different. The popular culture is different. The language is different. Et cetera, et cetera. Even for that small minority of people who do attempt to learn from the past, the superficial differences seem to blind us to the essential similarities with the past and render invisible the lessons that history so richly holds.

For cybersecurity professionals, the past can seem to be totally irrelevant. After all, there were no computers a hundred years ago. And in the rapid advance of technology, even the computers from fifty years ago are unimaginably primitive compared to the systems that now run the world. Without computers, and without modern interconnected networks, there were no phishing attacks, no denial-of-service attacks, no massive exfiltration of private data. There was no malware and certainly no ransomware. What possible lessons can the past hold for the modern cybersecurity professional?

The answer lies in the essential nature of security. Security has always been, and always shall be, a human affair. Security is 90%-95% psychology and sociology, and only 5%-10% technology. Over time, the tools have changed, but the nature of people has remained essentially the same. There have always been those who want to take from others. There have always been those who want to harm others. And there have always been, and always shall be, those who want and need protecting.

History teaches us that there are certain recurring patterns in the infinite cycles of attack, protect, attack, protect, attack, protect. One of the most common of these patterns is the tragic phenomenon known as "security theater". Security theater is the **appearance** of security without the **efficacy** of real security. It is an illusion. With security theater, there is always an essential element of security that is missing (Figure 1). At best, it can lead to a mild sense of false security. At worst, it can lead to disaster.

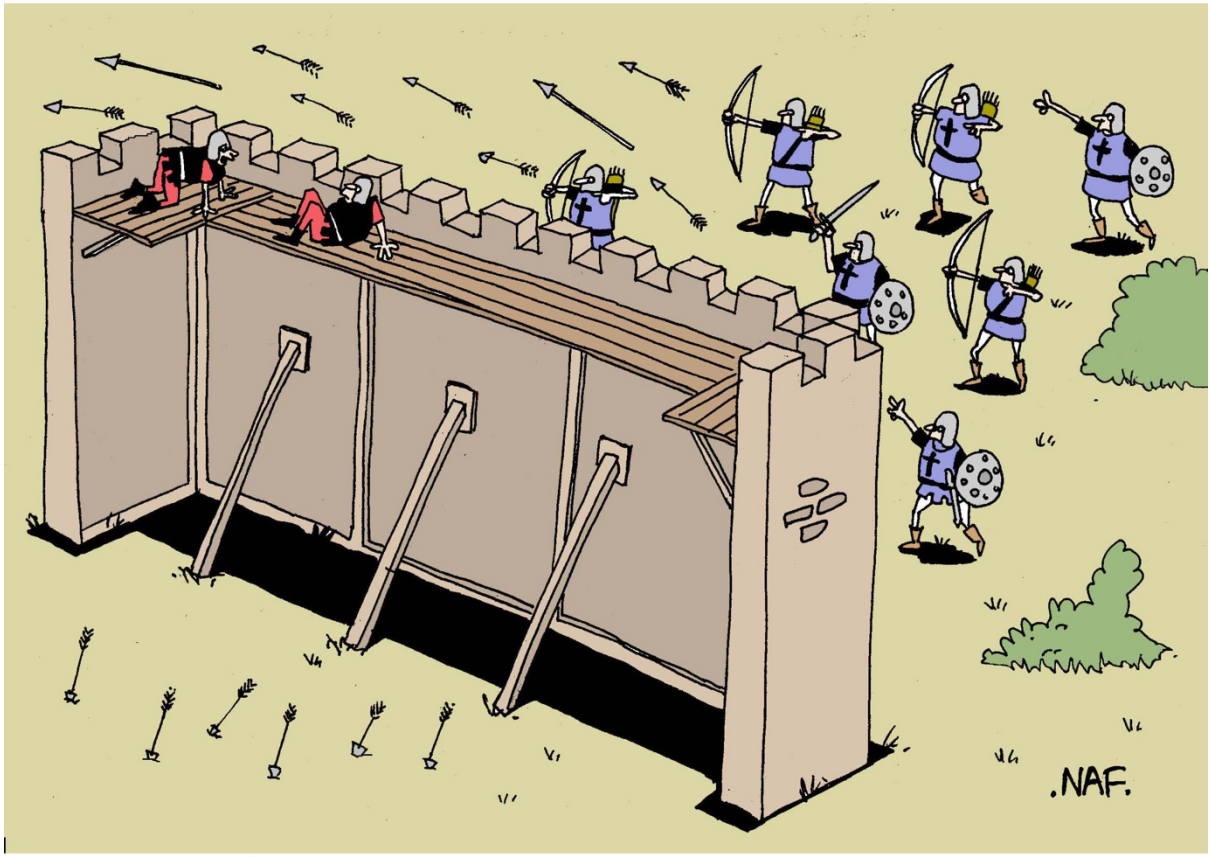
Imagine a bank whose building is built like a fortress (the appearance of security), but whose back door remains unlocked, and all the valuables are left lying around on the tables. Imagine a fortress designed to be impregnable, but one side of which is left totally unprotected. Imagine a massive wall, constructed using the most technologically advanced systems, designed to keep out a hostile enemy, but the wall does not cover the entire area to be protected. Imagine a large army prepared and trained to fight but using the weapons and the tactics of the previous war. Imagine a cybersecurity system that has all the latest technology but cannot detect many types of malware attacks. All of these are examples of

[1] "*Si Vis Pacem, Para Bellum*" Roman adage, adapted from Publius Flavius Vegetius Renatus, *Dē Rē Mīlitārī* :"*Igitur quī dēsīderat pācem, præparet bellum* ("Therefore let him who desires peace prepare for war.")

[2] Santayana, George, *The Life of Reason*, 1905

security theater. And in the latter instance, because "if you can't detect, you can't protect", it is an excellent example of cybersecurity theater.

Unfortunately, security theater is rampant in the world of cybersecurity. It is pandemic in its proliferation. Therefore, understanding security theater and being able to recognize it in all its various disguises, especially in the cyber world, are essential to establishing effective, real cybersecurity.



"We just have to hope and pray they don't go around the side!"

Figure 1 - Security Theater[3]

This whitepaper examines three historical examples of security theater, all drawn from World War II (WW II). It then provides analogs that are examples of cybersecurity theater, examples from some of what are generally regarded as the latest and greatest cybersecurity systems currently employed. Finally, it concludes with a few brief suggestions for how some of these instances of cybersecurity theater can, with minimal disruption, be transformed from "theater" to real security.

[3] CartoonStock.com

2. SECURITY THEATER: LESSONS FROM WW II

Studying history is especially informative when it comes to understanding security theater. History is replete with myriad examples. The following are from World War II and are paradigmatic. The errors that led to the very expensive and highly touted security efforts that turned out to be only security theater fall into three categories:

- Neglecting Unforeseen Factors
- Ignoring Previously Known Threats
- Preparing to Fight the Previous War

Neglecting Unforeseen Factors - Belgium and Eben-Emael

The massive fort at Eben-Emael was built by Belgium during the years 1931-1935. It was the premier state-of-the-art fortress of its era. Belgium, having suffered at the hands of the Germans in WW I, was determined to keep the Germans from ever overrunning the country again.

Eben-Emael "was designed to defend Belgium from a German attack across the narrow belt of Dutch territory in the region. … **it was reputed to be impregnable** [emphasis added] and at the time, the largest in the world."[4] Its walls were made of reinforced concrete many meters thick. It was surrounded by strong defensive topographical features, including tank traps.

> The fort is a colossal underground complex that extends over three levels and five kilometers of underground galleries. Its 17 surface works spread over 75 hectares constitute the centerpiece of the fortified belt of Liege. Similar to forts constructed by the French in the 16th century, Eben-Emael was built in the shape of a pentagon and is surrounded by an impressive array of fortifications against armored attacks.
>
> The fort was also equipped with special filters for the ventilation of combat gases.[5]

In early 1940, Eben-Emael's defensive contingent consisted of 1,200 soldiers. On May 10th, 1940, a mere 78 German paratroopers landed on its roof. One day later, the defenders of Eben-Emael surrendered.

What had happened? Why did this supposedly "impregnable" fortress fall so easily? The answer is that Eben-Emael fell victim to an unforeseen factor. Its designers and architects never considered the possibility of an infantry assault from the air. The roof, which was a very large flat grass-covered plain, was never fortified. It also provided the perfect landing field for assault gliders (Figure 2). Through the common error of assuming that all factors had been considered, Eben-Emael proved to be "security theater" rather than real security. Since it is

[4] Wikipedia: https://en.wikipedia.org/wiki/Fort_Eben-Emael
[5] Land of Memory: https://www.landofmemory.eu/en/sites-historiques/fort-eben-emael/

never possible to consider all possible factors, it is far better to be aware of this and remain vigilant in the face of the unknown. The alternative is to fall victim to hubris.

Figure 2 - The Roof of Eben-Emael – A Perfect Place to Land a Glider

Ignoring Known Threats - France and the Maginot Line

In 1939, the army of France was considered the most powerful in the world. It had a very large, very well-trained standing force. It also had an enormous standing reserve, similarly well-trained. This army was equipped with the most up to date materiel, including tanks that were regarded as superior to those of Germany and most other countries. In addition, it had its pièce de résistance, the Maginot Line.

Built in the 1930s, the Maginot Line was a 280-mile-long line of state-of-the-art fortresses protecting the entire border with Germany. These fortresses, connected by underground railways, were constructed to resist heavy artillery, poison gas, infantry, and tanks. They were equipped with underground hospitals, exercise gymnasiums, and even airplane hangars.

With the rise of Hitler and his NAZIs, Germany increased the size and the quality of its military. This was in violation of the restrictions of the Versailles Treaty[6], but at the time, the world did not react. In September 1939, Germany invaded France's ally Poland. England and France immediately declared war on Germany. However, the French military and its general population felt secure that Germany could not successfully attack France. France was simply too strong.

Few people at the time realized that France's defenses were merely "security theater". Even Winston Churchill, after visiting the Maginot Line in 1939 stated:

[6] The treaty that ended WW I. It placed onerous financial burdens on Germany and serious restrictions on the size and configuration of Germany's military.

> "The French front cannot be surprised. It cannot be broken at any point, except by an effort which would be enormously costly in life and take so much time that the general situation would be transformed while it was in progress."[7]

France's defenses gave the impression of providing very strong security. They inspired confidence, and they inspired confidence's evil twin: complacency. But they should not have. Despite France's large and well-equipped army, its military tactics were mired in the traditions and the modes of thinking left over from WW I.

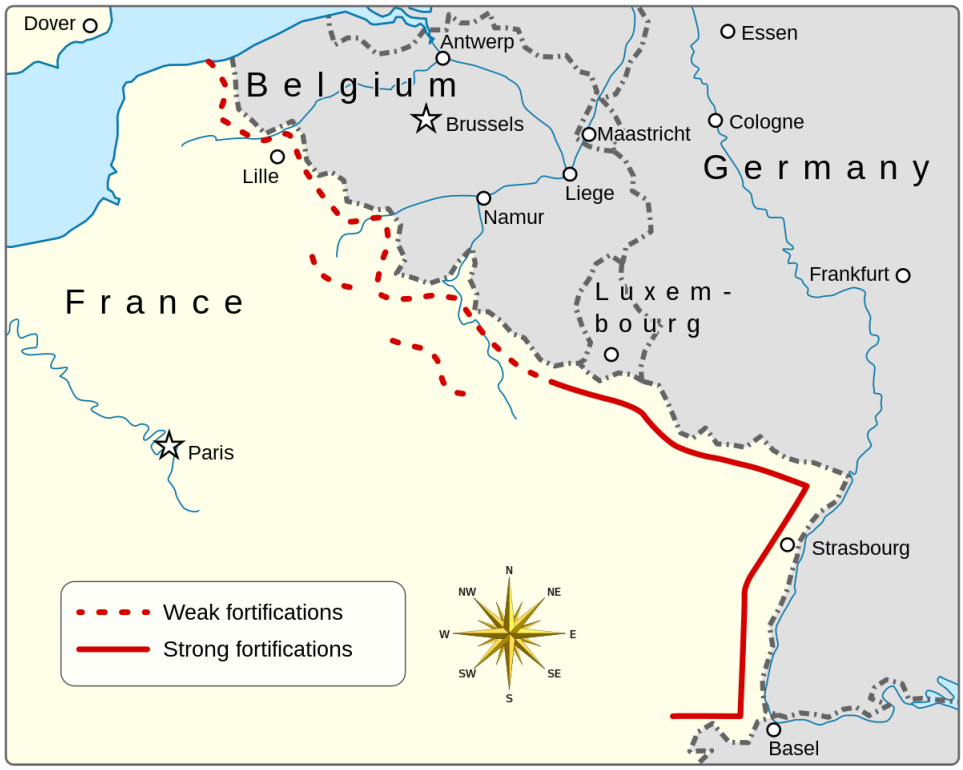


Figure 3 - The Maginot Line[8]

The Maginot Line suffered from two fatal flaws, both obvious to any astute student of history.

1. Fixed Fortifications: "Walls" have never proved effective in and of themselves. They are only useful in conjunction with other resources, including speed and mobility. They are useful only as temporary defensive positions. They cannot win a war. They cannot solve a problem. They have a tendency to appear to be a solution to a problem, when in reality, they serve only to hide the problem. As General George S. Patton stated after visiting the Maginot Line: "This is a first-class case of man's monument to stupidity"[9]
2. Ignoring the "Inconvenient": Prior to the outbreak of WW I, the bulk of the considerable French army was positioned on its border with Germany, essentially protecting the same areas as the Maginot Line did twenty-five years later. However,

[7] Addison, Paul, Winston Churchill (2007)

[8] https://simple.wikipedia.org/wiki/Maginot_Line

[9] Harkins, Paul D., When the Third Cracked Europe: the story of Patton's incredible army (1969)

in August 1914, the Germans relied upon a plan that had been in place since 1905, the "Schlieffen Plan". This called for the Germans to use an end-run around the French forces and attack through The Netherlands, Belgium, and Luxemburg (Figure 4).

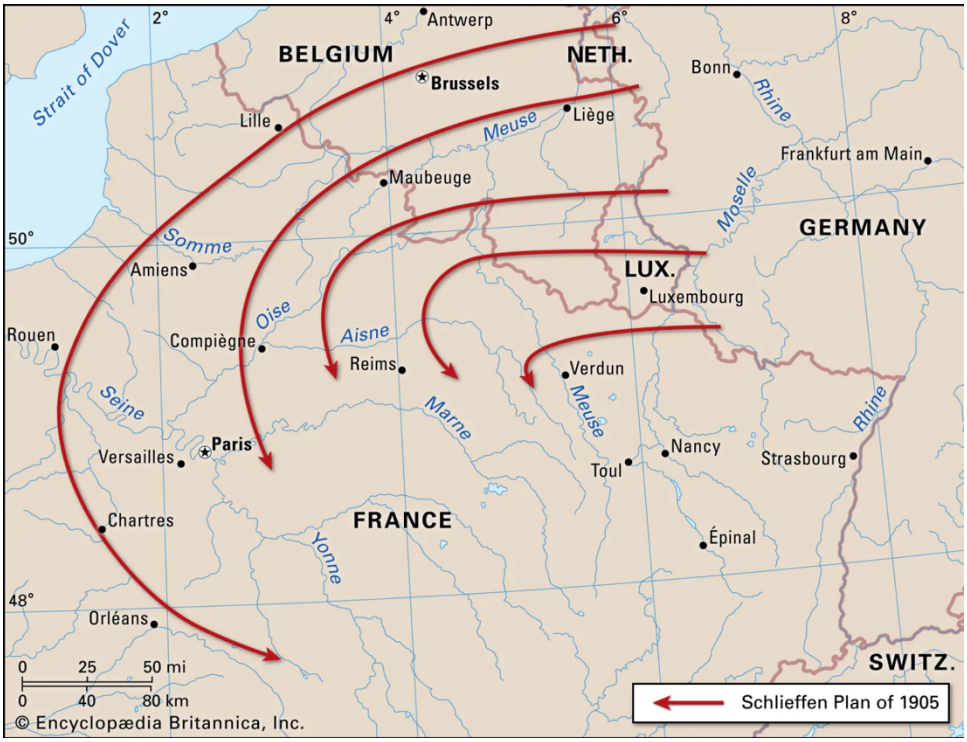


Figure 4 - The Schlieffen Plan[10]

The plan worked brilliantly. France almost fell in the first few weeks of the war. Only with the help of the British and later that of the Americans the tide was turned. After more than four years and millions of lives lost, Germany was finally defeated. An Armistice was reached in November 1918.

By the 1930s, when France was building the Maginot Line, the Schlieffen Plan was well known. Nevertheless, a repetition of that plan was not taken seriously into account in the design of the Maginot Line. The strong fortifications of the line were along the border with Germany (See Figure 3 above). Only far weaker and less dense defenses were set up along the border of Belgium and Luxemburg. Although France had suffered significantly from the Schlieffen Plan's almost fatal execution in WW I, and the leaders of France had all experienced the disaster, the vaunted Maginot Line was not constructed to prevent a Schlieffen Plan repetition.

Why not? Why was the Schlieffen Plan ignored when the Maginot Line was designed and built? The possibility of Germany again attacking through The Low Countries was an unfortunate and "inconvenient truth". It was something that the French politicians and military upper echelons were not willing to address. At best, the possibility of a repeat of WW I was given lip-service, but not treated with the priority it should have commanded. It was the proverbial large elephant in the room that those in authority chose to ignore.

[10] Encyclopedia Britannica, https://www.britannica.com/event/Schlieffen-Plan

Instead, the French leaders publicized the strengths and the innovations of the Maginot Line. No defensive line so sophisticated had ever been built. The technology was cutting-edge. Its rooms even had higher air pressure than the ambient air outside so that poison gas would not penetrate. Its soldiers were well-trained and there were sufficient numbers of them. In short, the French, and their allies, chose to focus on all the positive features of the Maginot Line, while ignoring questions regarding how well it could perform its basic function, its raison d'être: the prevention of the Germans from successfully attacking France.

On May 10th, 1940, Germany attacked France, and again did so using the principles of the Schlieffen Plan. The Germans once again came through the Low Countries and circled around behind the French forces. The French army and its magnificent Maginot Line were totally outflanked. Designed only to withstand a frontal attack, the Maginot Line failed miserably.

Preparing to Fight the Previous War - France and Its Large Army

As stated above, France had one of the largest, best equipped armies in the world, much larger than Germany's. Unfortunately, it was designed and trained to fight another WW I. In sharp contrast, Germany's top military minds (such as Heinz Guderian and Erwin Rommel) were building upon the theories of Alfred Von Schlieffen and even of the brilliant English military strategist B.H. Liddell Hart, developing the principles of Blitzkrieg: mobility and the integration of armor, motorized infantry, and air power. At the same time, the French were mired in the philosophy of defense. They looked to massive numbers of troops, defensive fortresses, and almost fixed-position tanks (more akin to semi-mobile artillery units than fast moving attacking cavalry).

In May 1940, the German panzer divisions sliced through the Low Countries. They encircled the British Expeditionary Force in northwest France and drove southeast to cut off the Maginot Line and the massive French army there. The ponderous French army could not move quickly enough nor efficiently enough to prevent its own annihilation. It was trained for WW I style trench warfare, not WW II blitzkriegs tactics.

The Results of Security Theater – Belgium and France Fall Rapidly

Germany launched its Western Front Offensive on May 10th,1940. Eighteen days later, on May 28th, 1940, Belgium surrendered. Less than three weeks after that, on June 14th, 1940, the Germans entered Paris. On June 22nd, 1940, France signed an "Armistice" with Germany that was essentially a total surrender. As an insult to France, the armistice was signed in the very same railroad car that the original Treaty of Versailles had been signed. On June 23rd, 1940, Hitler himself rode and strode through the streets of Paris.

Security theater is NOT security. It is only the illusion of security. Those who choose to rely upon security theater rather than upon real security are doomed to repeat the history from which they have not learned.

3. CYBERSECURITY THEATER: SOME EXAMPLES

Preparing to Fight the Previous War – Virus Signatures

The vast majority of malware detection systems rely upon databases of previously detected malware. These databases are primarily used in two basic ways:

1. Exact Code Matching ("Dictionary" Lookups): The malware detection system reads through the code being examined (e.g., a file) and looks for an exact match with any of the malware code examples, aka virus signatures, that reside in the virus signature database.
2. Code Pattern Matching ("Thesaurus" Lookups): The malware detection system reads through the code being examined (e.g., a file) and, using Artificial Intelligence (AI) pattern-matching technology looks for code that is similar to any of the virus signatures in the virus signature database.

This rearward looking approach has a number of serious drawbacks:

- Virus Signature Database Size: Current estimates now put the number of active computer viruses at over a billion. Consequently, the time it takes to compare each and every suspicious file to over a billion virus signatures is significant, and growing more significant as more malware arrives on the scene.

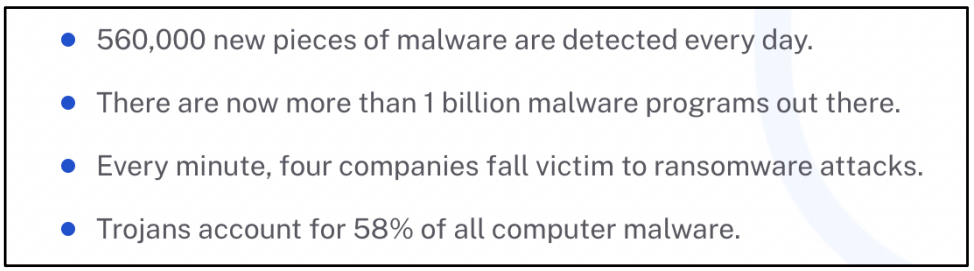


Figure 5 - Key Malware Statistics[11]

- Maintenance of Virus Signature Databases: In light of the number of new viruses continually appearing in the wild, maintaining up-to-date Virus Signature databases is an impossible Sisyphean task.
- Polymorphic Malware: Malware that can change its "signature" over time and location has, for many years now, been the modus operandi of both sophisticated cybercriminals and malicious state actors.
- "Zero-Day" Infections Are Undetectable: Malware that is truly new and innovative ("Zero-Day" Malware) is invisible to all rearward looking systems. Since their "signatures" have never been previously identified, neither a "Dictionary Lookup" nor a "Thesaurus Lookup" will ever find them.

Although studying the tactics used in previous wars can be very beneficial, it is only beneficial if one can extract and extrapolate the common factors of success and failure. These factors must be the abstract principles rather than the detailed specific technologies, modes, and

[11] DataProt, A Not-So-Common Cold: Malware Statistics in 2022, July 20th, 2022

methods. New technologies create new opportunities, but the general principles remain the same. History teaches us that fighting contemporary wars with previous wars' tactics is a rapid road to defeat.

Ignoring Known Threats – APT "Dwell Time" and Artificial Intelligence

Just as the designers of the Maginot Line included some of the latest-and-greatest technologies but ignored the manifest threat of a repeat of the Schlieffen Plan, many of today's very sophisticated and impressive cybersecurity systems ignore some very major and manifest threats. These threats are:

- Advanced Persistent Threats (APTs)
- Malware Detection Technology Already Known to Be Vulnerable

Despite the enormous significance of these threats, these, very much like the French reaction to the Schlieffen Plan, are given little more than lip-service. Usually, they are not even acknowledged at all. Speak to most cybersecurity officers and they will elaborate on the sophistication of their technology (much like the pride the French took in the Maginot Line's sophisticated technology). They will confidently tout the efficacies of their defenses. And they will never even mention nor consider the clear and manifest dangers of APTs and the questionable use of AI in their cyber defenses.

Advanced Persistent Threats – The Secret Enemy Within

Even a cursory examination of the recent spate of high-profile ransomware attacks reveals that the malware responsible for these attacks had resided undetected in the infected systems for many months, undetected by even "state-of-the-art" malware detection systems. These types of malware attacks, the ones that reside for extended periods of time within their target networks are known as Advanced Persistent Threats. They use their undetected time wisely, proliferating malicious code, collecting important attack data, and preparing for their eventual launch. When they are finally ready, they launch, usually with disastrous results.

Such advanced persistent threat attacks are not anomalous outliers, but rather more the rule than the exception. This is confirmed by numerous studies, not the least of which is the *Ponomon Cost of Data Breach Study 2022*. That study found that for systems which had fully deployed cybersecurity defenses in place, the average time to detect a malware infection was 181 days! That is essentially six months! (See Figure 6).

This time between infection and detection is known as "Dwell Time". Six months of Dwell Time for cyber systems is an eternity. Why are cybersecurity officers not more concerned about the clear and present danger that APTs present? Why are they not more focused upon reducing Dwell Time? Why are so many cybersecurity resources channeled into perimeter protection, at the expense of malware detection and remediation?

It is an often-forgotten truth that: "If you can't detect, you can't protect." Ignoring APTs will not make them go away. Relying almost exclusively upon perimeter protections will not prevent the APTs from penetrating. No wall is impenetrable. The APTs will get through. With no viable system to detect them quickly, they will succeed in wreaking the havoc they were designed to.

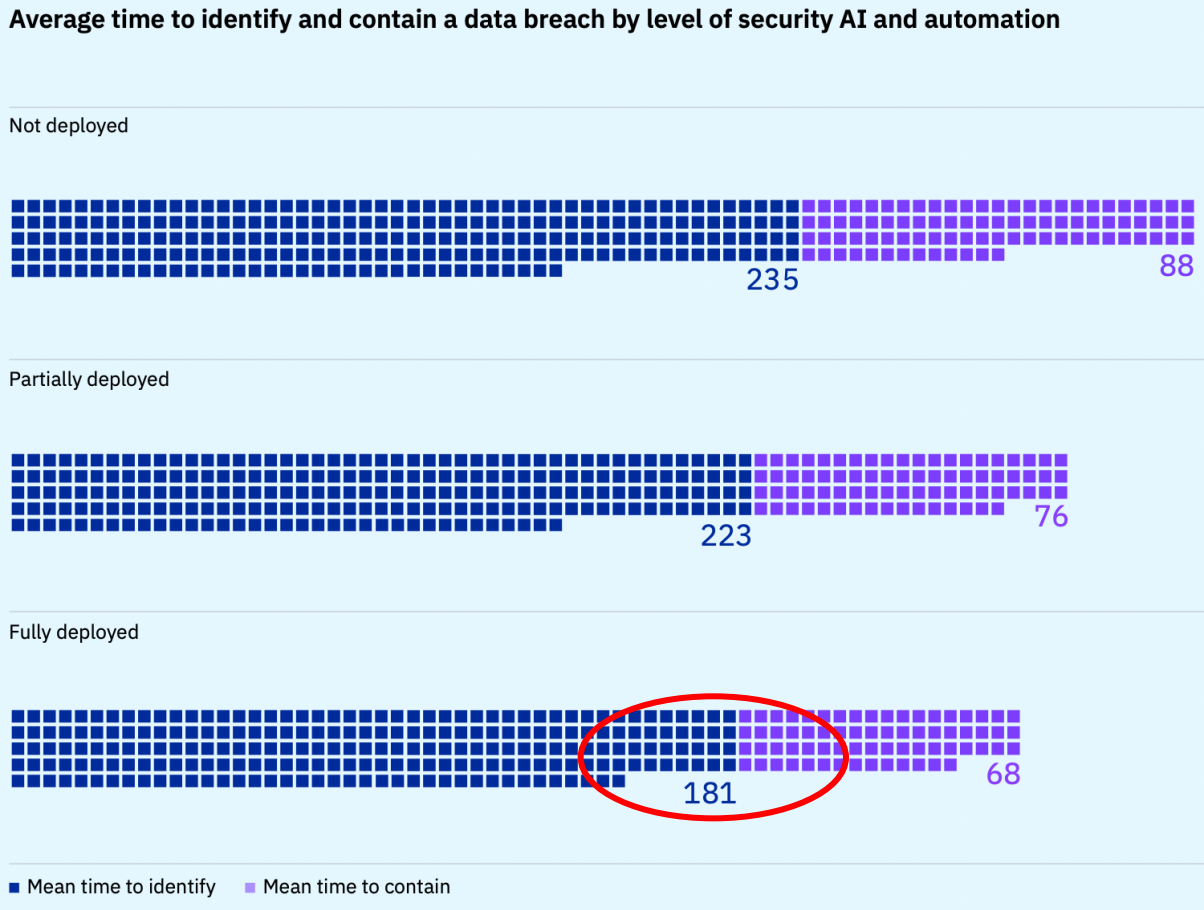


Figure 6 - Average Time in Days to Detect a Malware Attack[12]

Malware Detection Technology Already Known to Be Vulnerable

Just as Germany's ability to attack successfully through the Low Countries was known even before the Maginot Line was built, that is, the Schlieffen Plan, so too are there malware detection technologies employed today for which an obvious way to circumvent them exists. For example, consider the technique known as "Sandboxing".

> A sandbox is a protected cell within the computer the anti malware creates to contain any suspicious or unknown file. This prevents malware infection because the file runs without infecting the other programs in the computer.
>
> Inside the sandbox, the file is observed and analyzed further to determine if it's harmful or safe. If the file is legit, it is released, but if it's malicious it is denied.[13]

At first glance, this may seem to be a very effective bulwark against malware infections. But what is the obvious circumvention? Time-delayed malware attacks. Hide a malware attack inside an innocuous file, and have that attack launch in a week, or month, or even a year later.

[12] Ponomon (IBM) Cost of Data Breach Study 2022
[13] Comodo Cybersecurity, enterprise.comodo.com

How long can the sandbox hold a suspicious file before that file must be released? Using time-delayed malware is an obvious circumvention to sandboxing protections.

Reliance Upon AI to Detect Malware – The Double-Edged Sword

This same type of known circumvention exists for a far more ubiquitous malware detection technology: Artificial Intelligence. Artificial Intelligence has been the darling of the cybersecurity industry for over a decade. There is no question that AI is an umbrella term that contains many powerful and useful tools. Are some of these tools very useful in cybersecurity? Yes! A resounding yes! Are they useful in the direct detection of malware infections? Despite a massive industry trend that says that they are, the answer is no!

AI is a double-edged sword. The cybercriminals and malicious state actors have access to exactly the same AI technology and AI expertise as the cybersecurity companies; and they are usually better funded. AI can be used to attack as well as to defend. The result of using AI as a detection engine is an endless AI arms race of AI defensive tools battling AI attack tools. Such an infinite arms race, one in which the attackers can afford to lose often, but defenders cannot afford to lose once, is not a viable cybersecurity defensive strategy. It is a recipe for disaster.

Two of the areas that AI is currently for malware detection are:

- Pattern Matching – To find polymorphic malware, that is, malware similar to malware that has been previously seen and identified.
- Behavioral Anomaly Detection – To find network behavior that is different from "normal" network behavior. As one vendor advertises on its website:

> [Our] Self-Learning AI understands what makes you unique - every user, cloud account, desktop, laptop and server. Understanding your organization's version of normal is the key to detecting everything that's not.

The problem with Pattern Matching is that, despite years of use, it is fraught with a plague of false positives. Some studies estimate that the costs of these false positives exceed those of most malware attacks. In order to ameliorate the collateral damage caused by the false positives of AI pattern matching systems, some cybersecurity vendors now use human analysts to filter their raw "detection" data before passing it along to their customers. This helps but is both very expensive and not nearly effective enough. The AI that the cybercriminals can use to disguise their malware can eventually defeat all the AI systems designed to find the malware patterns in the chaos.

The problem with Behavioral Anomaly Detection is that the world of system behavior is dynamic. It is not static. It is constantly changing. Thus, the Behavioral Anomaly Detection systems must be able to learn certain acceptable changes and incorporate them into their canon of acceptable behavior. As such, the Behavior Anomaly Detection systems must constantly be learning. They must constantly be adapting to the, sometimes subtle, changes in the protected systems' behavior. As one cybersecurity vendor advertises:

> We could call our Self-Learning AI the most powerful of its kind but the truth is, there's nothing else quite like it.

> It doesn't just learn your organization, inside and out, down to the smallest digital details. It actually understands what's normal to identify what's not.

But if the system must learn, and it must, it must therefore be able to accommodate small, "insignificant" changes and accept them as "normal". It cannot treat every change, no matter how minor, as being an attack. Otherwise, it would drown in an ocean of false positives. Thus, if a very patient, very sophisticated, AI-based attacker "had … world enough and time", it should be able to examine and analyze a "target" system, and then introduce a long series of "insignificant" changes that would train any Behavioral Anomaly Detection system to ultimately accept as normal almost any desired malicious behavior.

The dangers inherent in relying **only** upon AI algorithms for malware detection are too obvious and too critical to be ignored. And yet, as the French prior to WW II ignored the possibility of a rerun of a Schlieffen-like plan, most cybersecurity professionals today ignore AI's blatant vulnerabilities. Like the French glorifying in the technological sophistication of the Maginot Line, today's cybersecurity firms glorify themselves and their products in the apparent sophistication of AI.

Neglecting Unforeseen Factors – Complacency & Willful Blindness

"Eyes they have and will not see. Ears they have and will not hear"[14]. Willful blindness is a common occurrence, and older than the Bible. The designers of Eben-Emael knew about airplanes, gliders, and paratroopers. They were, however, so focused on the battles and tactics of WW I, they never stopped to consider how the new aerial technologies might be used in future wars. Similarly, in the world of Cybersecurity, the dangers of complacency and over-confidence are very well understood.[15] Nevertheless the competition to sell cybersecurity products and services is so great that it prompts over-zealous vendors to make outlandish and unsupportable claims. These claims are designed to win over customers. Unfortunately, they have the added effect of creating negligence-inducing over-confidence in those same customers.

Techno-babble – The proliferation of essentially meaningless terms

Consider some of the terms used today to market cybersecurity products:

- Zero Trust: If one simply and uncritically reads the phrase "Zero Trust", it would seem to imply something that is inimical to, if not impossible for, computer systems. If there is zero trust, then there can be no communication whatsoever. Some level of trust must exist. There must be, at the very least, some trusted parties. And indeed in practice, "Zero Trust" implementations do not really mean zero trust. "The concept of Zero Trust … recommends that organizations should never trust any entity, and should verify every user or device before granting them access to sensitive resources."[16]

[14] Jeremiah, 5.21 "עֵינַיִם לָהֶם וְלֹא יִרְאוּ, אָזְנַיִם לָהֶם וְלֹא יִשְׁמָעוּ"

[15] See Crytica White-Paper: The 3Cs: Enemies of Cybersecurity

[16] Menlo Security, The Ultimate Buyer's Guide: Zero Trust Network Access, p. 4., 2022

That is a very sound concept, one that should be perhaps universally implemented. However, it should not be called "Zero Trust". The inaccurate name gives a very false impression of what the principle is. Perhaps a more suitable name would be "Verified Trust".

The misleading name of "Zero Trust" has led to numerous articles in the trade publications attempting to clarify to would-be adopters of this principle, that Zero Trust does not really mean "zero trust". Why use an essentially meaningless term that sows confusion when perfectly clear and concise terminology does exist?

- MDR/XDR: Managed Detection and Response / Extended Detection and Response are terms very similar to "Zero Trust" in that their principles are sound, but their terminology over-promises. Their names imply an ability to "detect" attacks rapidly and actionably, to detect attacks with a speed and efficacy such that appropriate and timely "responses" can, and shall, be forthcoming. As noted in Figure 6 above, the average time for a fully deployed cybersecurity system to detect a malware infection is greater than six months. If that is so, then the acronyms MDR and XDR are almost meaningless. How can there be an appropriate response when the "Dwell Time" (the time between infection and detection) is over six months? The concept of managing and coordinating detection and response is an excellent one. But using language that implies that it is being accomplished is, at best, misleading.
- Proactive Protection: "Proactive Protection – … to help you stay ahead of attackers and defend your environment." The implication being that it **is** possible to provide "Proactive Protection". The word proactive means: "taking action by causing change and not only reacting to change when it happens."[17] What does "proactive protection" mean in the context of cybersecurity? Is there actually a way to change malware, or attack malware, before it ever attacks a protected system? In the military, there is the concept of a "preemptive strike". That is a proactive operation. It is an action taken to prevent an enemy's action. With malware, however, it would seem that the only "proactive" actions one can take are to be prepared with solid detection and remediation mechanisms. Is the preparation of detections and "reactions" being "proactive"? Possibly. But that is not what is usually implied by "Proactive Protection".
- SideScanning™ Threat Detection: Side scanning radar and side scanning sonar are very well-established technologies. They can create very detailed and multi-dimensional images of the areas that they are scanning. The name is derived from how the radar/sonar is employed, scanning from multiple locations in order to integrate the resulting multiple views into a well-defined multi-dimensional image. But in what way is SideScanning™ computer threat detection "side scanning"? Do the scanners rotate around or travel past the systems they are scanning? Are they using multiple vantage points to establish multi-dimensional detection maps? It is far more likely that the term is employed because it evokes images of sophisticated technologies, without any real relevance to the actual technologies being used. It

[17] Cambridge Dictionary

exists primarily for a marketing effect, not for accuracy.[18] The result is yet another meaningless term that clouds the space rather than adds to clarity and understanding.

- Artificial Intelligence (AI): For most people, the invocation of AI is the equivalent of invoking the Good Witch Glinda from the Land of Oz. The impression is one of magical powers, being employed on the side of "good". However, exactly what those magical powers are and how they are used remain a mystery. As discussed above, AI can be a very powerful tool, but its use is not only limited to "the good guys". It can be used equally as effectively for evil. Invoking AI as a marketing term for cybersecurity creates an air of exotic mystique, but it communicates very little of substance. Its use almost inevitably creates a false sense of security in those who should not at all be feeling secure.

These are only a small sampling of the essentially meaningless terms that have taken root in the cybersecurity lexicon. They serve only to add to the mystique, to add to the confusion, and to render consumers more vulnerable to the claims of snake-oil salespeople. Even worse, they help to create a culture of over-confident complacency in an environment that requires the utmost vigilance.

Techno-Hype – The proliferation of dubious claims

A direct consequent of cybersecurity's arcane aura and magical mystique is that many dubious claims, unfounded claims, and even bold-face lies are promulgated unchallenged. Very few people are qualified to cut through the techno-babble, to understand the mundane reality behind the magical terminology. This leaves the marketeers free to prey upon the credulity of an audience eager for a cure for the malware pandemic.

Just a few examples of this type of techno-hype are found in the following ads:

- "**Ransomware protection can be as easy as 1-2-3**. Secure your email, web apps, and data with [redacted]."

  Really? Ransomware is still a major cybersecurity threat and remains so long after this ad first appeared. If this vendor truly had the cure for ransomware, why are ransomware attacks not being stopped?

- "**[We provide email] Attachment Protection** - [redacted] combines behavioral, heuristic, and sandboxing technologies to protect against zero-hour and targeted attacks. A sandbox environment is used to detonate and observe behavior of suspicious attachments."

  As noted above, there is an easy way around sandboxing (using time-delayed attacks). However, the bigger concern here is how can one protect against malware embedded in encrypted attachments. Without decrypting the attachment first, there is no way to detect what is contained within the attachment. But unless a user wants to give a

[18] It might be argued that because the SideScanning™ systems scan from a separate computer, and not from the computer being protected, the scanning takes place "from the side". That would be, at best, a spurious argument. In addition, the concept of being able to scan remotely, using no code on the scanned computer, is regarded by some as being as "spooky", as Einstein's "spooky action at a distance", and should not be conflated with the sophistication of side scanning radar/sonar.

cybersecurity system access to its confidential, encrypted information, and to its encryption/decryption keys, the claim of being able to protect against all email attachment attacks is bogus.

- "**Phishing and Impersonation Protection** - Automatically detect and prevent impersonation, business email compromise, and other targeted attacks. [redacted]'s AI engine learns each organization's unique communication patterns and leverages these patterns to identify anomalies and prevent socially engineered attacks in real time."

  Once again, relying upon AI to identify sophisticated phishing attacks is iffy at best. Faced with an attacker's AI phishing engine, this vendor's AI would quickly be outgunned; not to mention the plague of false positives that would most likely result. The questionable performance of most SPAM filters should quickly illustrate how unfounded this vendor's claim is.

- "**Antivirus, anti-malware, anti-spyware, anti-phishing, anti-ransomware, browser protection and more**. - [redacted] products include multiple defenses against viruses and malware. Our technology is powered by artificial intelligence (AI) and machine learning, and we are part of one of the world's largest civilian cyber intelligence networks."

  A basic tenet of cybersecurity is, and remains: "If one cannot detect, one cannot protect." And yet, despite all the cited impressive technologies in use by this vendor and others, the average Dwell Time, the time between infection and detection, for systems using all these fully deplored technologies, is over 180 days. Thus, how can this vendor claim all the protections it purports to provide if it cannot even detect malware in a reasonable, actionable, period of time?

- "**Safe from all new and existing threats** - Spending more time online can expose you to numerous cyber-attacks. [redacted]'s multi-layered protection keeps your documents, pictures and videos safe from all known and emerging threats, including ransomware, malware."

  This same vendor, in other locations and documentation, admits that they do not detect "all" threats. That is not, however, the impression given by the bold claim that their users are "Safe from all new and existing threats." Why then, the misleading, inaccurate, and untrue claim?

All the cybersecurity vendors quoted above do provide truly very valuable cybersecurity services. All are well-known, well-recognized, well-regarded companies. However, their dubious claims and advertising deceptions are highly counter-productive to cybersecurity.

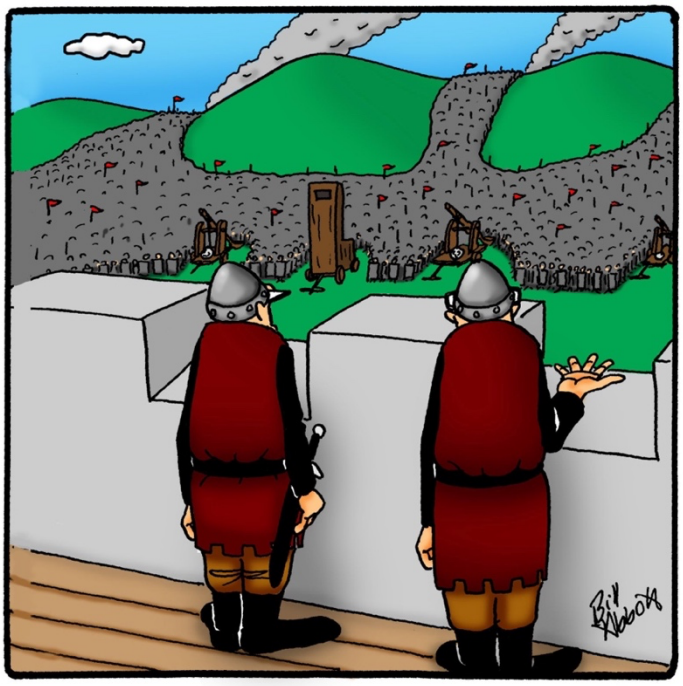
All security demands realistic assessments of the threats and dangers. All security requires awareness and vigilance. Cybersecurity is no exception. However, the marketing practices of many in the industry sow counter-productive complacency and exhibit tragically willful blindness. These are the classic hallmarks of security theater.

4. CYBERSECURITY THEATER – WHAT CAN BE DONE?

Since security theater is so manifestly self-defeating and self-destructive, why is it so prevalent? The answer to that question is complex. It pertains to the fact that security is primarily a question of psychology and sociology more than it is of technology and equipment. Security is a function of awareness and vigilance.

Therefore, true and effective security requires widespread awareness and vigilance, which in turn require that cybersecurity companies be forthright and honest in all of their dealings with the public. End-users must be educated. They must be knowledgeable enough to take an active part in their own security. They cannot be relegated to the role of non-thinking robots, nor lulled into a false sense of security by hollow phrases and meaningless promises. Cybersecurity solutions must be explained so that the end-users can understand them and use them as they should be used. The technology should not be hidden in a cloud of arcane jargon and mysticism.

The purveyors of cyber services must not promise security that they cannot deliver. For example, consider the web browsers that allow the user to set a "Do Not Track Me" flag. Websites seeing that flag still have the option of ignoring the flag and tracking the end-user. They are merely "requested" not to.



"Well, so much for the 'No Trespassing' signs."

Figure 7 - An Analog to the Do Not Track Me Flag[19]

[19] CartoonStock.com

The request not to track is totally unenforceable from the end-user's point of view. The "Do Not Track Me" flag is yet another example of cybersecurity theater. It provides the end-user with the illusion of being in control, of having a defense, when in reality, it does not exist. The "Do Not Track Me" flag is the modern-day analog to the image in **Error! Reference source not found.**

The Romans knew that "If you want peace, prepare for war." If you want cybersecurity, true cybersecurity, you must be prepared for the inevitable cyber-attacks that are coming. For those preparations to be effective, they must consist of real security measures, not merely security theater.

5. CRYTICA SECURITY – A DIFFERENT APPROACH

Crytica Security is an example of one cybersecurity company that does empower its end-users. It does not claim to be all-things-to-all-people. It does one thing only, malware detection, and it does it very well. Its functions are well defined and explained. Its principles are easily comprehensible, even by the least technology sophisticated users. Its marketing position is not to compete with other cybersecurity vendors, but rather, to work synergistically with them and strengthen them.

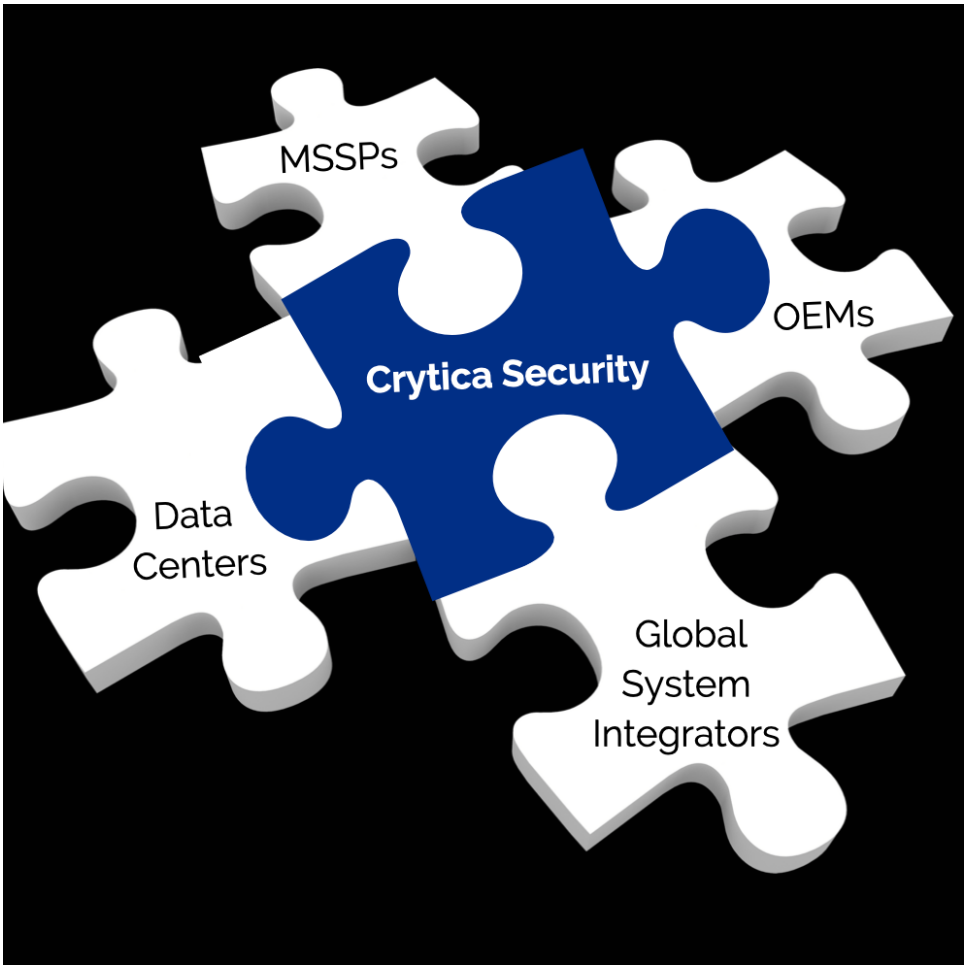


Figure 8 - Crytica is the Missing Piece

Crytica is an effective malware detection engine, one that reduces the APT Dwell time gap, from months to minutes. It can even detect Zero-Day malware injections. It is a deterministic engine, not a probabilistic (AI) one, so that false positives are not an issue. And, very importantly, Crytica works cooperatively with other systems, so that it can easily be integrated into a vast array of environments (Figure 8).

For more information on Crytica's non-theatrical malware detection solution, contact Crytica Security, Inc.:

Website: CryticaSecurity.com
Email: info@cryticasecurity.com