Welcome to the AI Powered TSM Cyber SCIF (CS)

Does there exist a means to neutralize ransomware?

Turns out there is. And it's not as far-fetched as we think. In fact, most people in cyber security already know a way to do this. And with the power of AI, it can be utilized more effectively than ever.

If we look at recent ransomware attacks, there's a model that shows us how to neutralize ransomware to the point where attacks can be addressed quickly with no need to pay a ransom.

"Sometimes a disease's greatest strength is also its greatest weakness."

We know that when ransomware attacks take place, it is usually based on a system exploit or vulnerability. Because finding and compromising these vulnerabilities is typically automated, the same exploit is often replicated by other ransomware actors in succession.

In this scenario, the very first ransomware outfit that gets through will be able to pull the data out in a readable format and then lock all the information in the compromised system. Let's call this group 'Attacker 0'.

So where is the answer for ransomware?

Turns out, our answer can be found in what happens after Attacker 0 strikes…

Once the compromised system is encrypted, all subsequent attacks typically find an entirely different reality compared to Attacker 0. This is because any later ransomware groups are, in fact, pulling already encrypted versions of the sensitive information - which renders their prize useless to them. It is locked with a key to which they do not have access. They are, in effect, neutralized.

While this is not necessarily good news for the client that's been attacked, the fact remains that all but one of the attackers are rendered ineffective.

Can we use this knowledge to neutralize all ransomware - including Attacker 0?

Yes we can…

“Most successful inoculations actually use the disease against itself by exposing the host to the disease to train the host to be immune to it.”

The TSM Cyber SCIF can do to Attacker 0 what Attacker 0 did to all other attackers. In effect, we become Attacker 0 (or perhaps Attacker -1) with the major difference being we (along with you) are the ones in control of the key and therefore dictating terms.

We have inoculated ourselves. While it is not necessarily prevention, it is immunity.

In essence an Attacker 0 who is your partner, not your advisory.

But can this be accomplished in a way where resources can still do their work?

“The cure cannot be worse than the disease.”

The good news here is that TSM combined with AI means the answer to this question is: “Yes you can!” - in a big way.

By incorporating AI technology into the Cyber SCIF, TSM can take secure information processing to a whole new level - automated text scraping, audio recognition, visual recognition, matching and identification, tabulation and more.

And just like with Vegas - what happens in the Cyber SCIF stays in the Cyber SCIF. Any responses are limited to not allow exposure of anything compromising - just like with a traditional military SCIF.

Some companies claim that they are already doing this by storing keys separately from the data. And often they employ elaborate mouse traps to make it harder for accounts to access the key to combine it with their data. There is, however, one striking difference between this approach and what TSM offers - if an automatic process exists where the key can be made available to access the data (even if only for super admin accounts), then this is fundamentally different than our ransomware attack scenarios and also fundamentally different than the TSM Cyber SCIF.

And with the power of AI, access to your data can be separated from access to your information. For example, records can be tokenized in the CS to reveal only necessary business metrics on important trends that need to be addressed - business information returned without exposing data. AI does not care that records are tokenized and it doesn’t care about the format of the information itself (like if it is encrypted or not).

Think of the CS as AI with the power to run very advanced processes without super admin account access or any other type of back door.

A partner that can tell you if there are important issues to address, and then safely guide you to where to go to address them. An Attacker 0 level lockout where you dictate how the information is leveraged.

Let's look at some of the advantages the TSM Cyber SCIF offers in addition to protection against ransomware…

1. Immunity against insider threats
2. Immunity against data breaches
3. Immunity against sabotage
4. Immunity against 3rd Party and Vendor exposures
5. Greater system recovery
6. Zero Trust Compliance
7. Reduced reliance on front-line personnel for security
8. Greatly improved forensics
9. Enables End-to-End Encryption (E2EE)
10. Integrates with existing systems
11. Helps business focus more on the business

Is it all roses?

Would you turn over your data (or parts of it) knowing you (along with everyone else) could not directly access it again without significant procedural intervention? Would your answer change if you knew you could always get required information without risk of exposure?

New approaches require new ways of thinking and working. Different does not have to be a bad thing. In fact, in perhaps the most important area, this can be an exceptionally good thing.

"The news you want to hear from your doctor is that the test is negative."

TSM helps put you on the side of the great news from Doctor FBI.

Because the key is not available, the FBI can certify after an attack that no breach has occurred. With this news, organizations can resume operations much more quickly and have greater control over next steps, payment amounts (if any), and schedules.

What is our sanity worth?

We know that the definition of insanity is doing the same thing over and over and expecting a different result. If the current approach to protecting sensitive information was working, then in all likelihood we would not be reading this.

There is a way that we can readily see does work. The AI powered TSM Cyber SCIF (CS) can get you there!

info@JJDSoftware.com
https://ternarysecuritymodel.com/