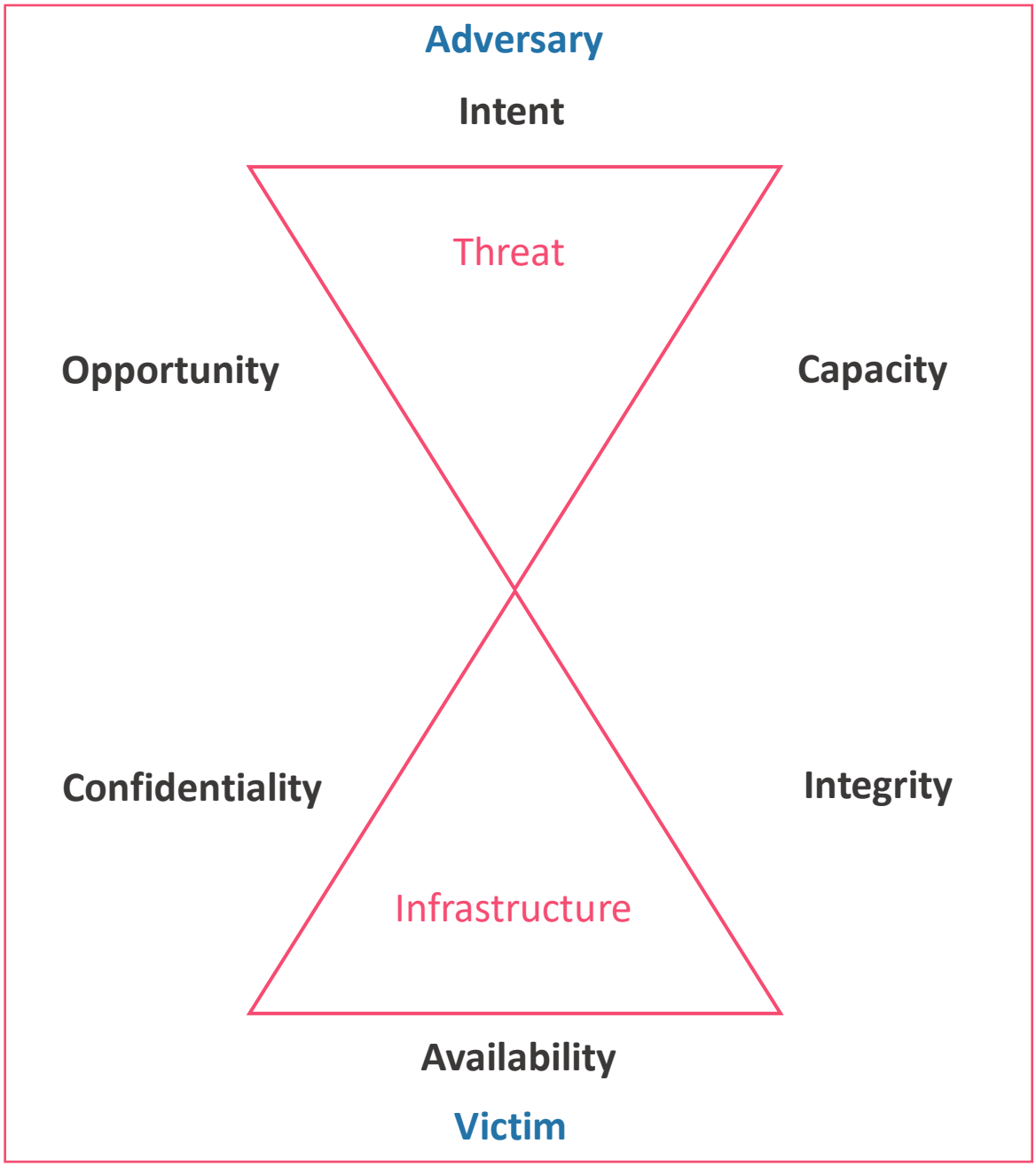
The "Sand Clock" Model of Cybersecurity

Javier Stransky


Adversary
Intent
Threat
Opportunity
Capacity
Confidentiality
Integrity
Infrastructure
Availability
Victim

“If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle.”

— Sun Tzu, The Art of War

Introduction

If we go back in time, talking about cybersecurity, we would probably find ourselves discussing about which Anti-Virus and firewall where the best or "more secure", with probably not even a real security strategy. Two decades ago, that was not as bad as it looks today. The threat landscape changed a lot, along with the size of the internet, the business models, how we work and not exaggerating, the minds of an entire generation. So now, we cannot survive as an organization without a proper security strategy, of course with the right -and necessary- investment.

That's something that we are going to hear on any cybersecurity conference and webinar around the world for sure, but the question now is

¿Why?

When the business models decided to take a posture more technology-oriented, the impact surface on every organization became wider. But not everything was money-related, since the development of new technologies allowed to increase productivity and commodities everywhere. This meant that all humanity voted for technology and its benefits, including new job roles that increased the use of computers, programs and internet. ¿So far so good, right? Well, not so much. The problem that came with this, is that with a bigger fortress to defend we needed more security-oriented technology investments, human talent, policies enforcement and so on, but the vast majority of companies worldwide didn't take this seriously enough.

Over the past 2 years, let's say, since the COVID-19, we found ourselves working almost entirely remotely, which increased the demand of internet

usage, web applications, cloud services, e-commerce and, along with this, a rise of at least 300% in cyberattacks.

The thing is, not only the companies, organizations and government moved to the internet, but also the criminals and terrorists. Now, it's not just about adding the prefix "cyber" to what they are. They found their way to know how to disrupt business continuity, conduct industrial and government espionage and make real money raising an entire business model with the exploitation of Ransomware and information leakage. According to Kaspersky recent reports, only in the past 6 months, they found 'a couple millions' of Ransomware's reported cases.

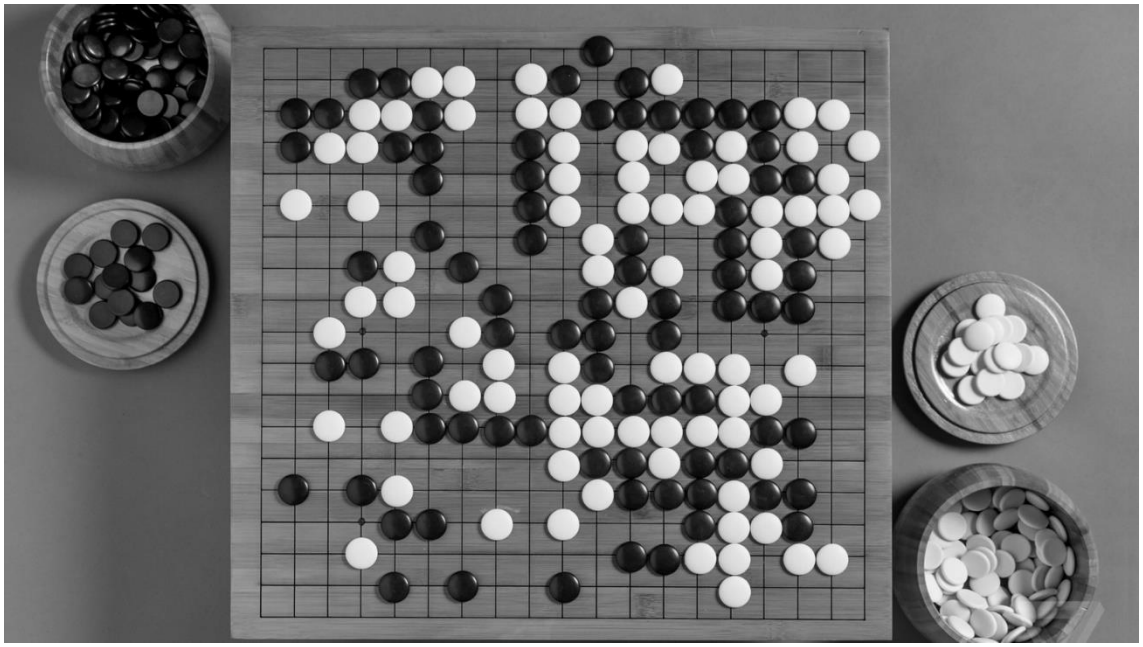
Regarding Cybersecurity analysts, we had to learn not only how to secure an infrastructure and its private information using more sophisticated technology like Machine Learning tools, XDRs, etc. But also, we had to create more complex security models, and raise the bar. We had to become *Generals* and *Warriors*.

As we kept learning how to repeal more advance attacks, we reached a certain point where the hacker at the other side of the table, needed to be seeing as an *"Adversary"* like if we were dueling. This posture began when we started analyzing "threats" and "adversaries" like a military-Intelligence would do. We understood this as a continuous never-ending war, so we had to take a military approach to accomplish this, since we were facing more advance threats, or as we call them "APTs" for Advanced persistent Threats. This is were the concept of "*Threat Intelligence*" began to take a huge relevance on any security conversation. Taken mostly from the department of defense and the CIA from the US government, we absorbed and implemented concepts like the Intelligence Cycle.

Some of the most famous models that are used on the entire industry to understand cybercriminals and their behavior are the "*Cyber Kill Chain*" from Martin Lockheed, the "*Diamond Model*" from David Castiglione and the MITRE ATT&CK framework for Tactics, Technics and procedures (TTPs). All of these models are intelligence-based and describe the behavior of and adversary during the entire process of compromising an entire network.

Of course, a lot of this security strategies and mindsets have been here for a while, you can take "The Art of War" as an example (written more than 2000 years ago), but we began to actually use it on this field around a decade ago, mostly as a combination of military and security intelligence agencies. Although, it had its own evolution and it keeps changing constantly to adapt our security needs, it's not strange that new models show up based on the previous ones, trying to close the gaps or point it out a different approach.

In other words, that's why I'm here today, to explain a security model I came while I was trying to demonstrate some Threat Intelligence concepts. I think this might be quite simple for cybersecurity experts, but it might be useful for the ones are not. To circle up, saying that something is simple, doesn't mean it's not effective.



The Sand Clock Model

Planning for the cybersecurity of an organization has put some light on concepts that any CISO, Security Manager and/or Compliance Security Officer must know, in order get the expected results. Between all of these, there's one that probably stands up among the others, which is the cybersecurity "CIA Triad". The CIA name comes from "Confidentiality", "Integrity" and "Availability", concepts that we will explain one by one and then as a whole.

Confidentiality

The concept is to prevent unauthorized access to restricted and/or private information. As its name points it out, keeping information confidential works for governments, companies, healthcare organizations, banks, and even you, as an individual. When this kind of right gets compromised, the security of a nation gets threaten, the trust on a company falls (which is obviously bad for business), and it also means that something potentially valuable has been stolen from us.

The way we ensure this confidentiality, can come in different ways, since it might depend if you need to get line up with a security policy like GDPR, ISO 27000/270001, HIPAA, etc. It can also come as best practices, like the ones recommended by NIST or the CIS Controls.

Integrity

Protect Information from being modified or destructed. There are a lot of cases when we need to make sure that something like messages, programs,

files has not been tampered. Imagine that in a hospital environment a 'Script Kiddie' decides to change medical records from a database, that would be terrible ¿right? or if in any government confidential report whose content might depend an important decision, a hacktivist changes the content just to create chaos. ¿Can we measure the size of these possible catastrophes?

In any case, using methodologies like hashing comparison, signature approaches and keys, we found a few ways to make sure that files, programs and messaged have not being manipulated.

Availability

Availability in this case is a synonym of reliability and trust, which means to ensure that a service keeps up and running no matter what happen. Of course, this is closely related to strategies like 'high availability', 'resilience', 'disaster recovery', 'backups' and 'redundancies' among other things, all that falls into the infrastructure and network planning. But there's a lot of space for cybersecurity in this domain, since we still need to ensure that DOS, DDOS, flooding attacks and so on, does not disrupt business continuity. For sure, there are a lot of other reasons, these are just an example. Let's imagine that we have a webstore and business is going well, so well that our competency tries to take down are sells during the "*Black Friday*" and for that, they use one of the mentioned attacks. ¿Are we ok with losing all the money, because we didn't have the right security implementations in place to prevent this to happen? I think not.

As a Whole

Now that we have a basic understanding of these 3 sides of the triangle ¿what does it mean as a whole? The sum up of these security-aware approaches consolidates how we structure not only the way we manage

information and our defense posture, but also gives us a security-oriented infrastructure disposition. In other words, the whole architecture has to be done with cybersecurity and cyber resilience in mind.

Know yourself

If you read the quote from page 2, which is from "*The Art of War*", it's not just something that I put there because its cool, I use it because it's the perfect explanation for us to understand both sides of the clock. "Know yourself" means to be aware of every node, network, application, port, etc. that is right there inside your infrastructure. Not having knowledge of what is your current surface of attack, implies that you're already vulnerable.

You wouldn't believe how many attacks happen everyday and success because of exposed services, protocols and ports to the internet, a lot of these happens without the knowledge of the system administrators. Yes, employees might change over time and some technical details are not handover properly, but the organization needs to implement strict documentation procedures of the entire topology, policies, regularly test for vulnerabilities, educate the users and patch as much as they can.

There is another type of information regarding our organization that will not necessarily be found inside our infrastructure, which is the public information out there on the surface-web, deep-web and dark-web. Today, using OSINT (Open Source Intelligence) methodologies like any threat actor would do during the "Recon" phase, we can gather a lot of details from employees, their positions, emails, old leaks, company structure, metadata, web services and so on. Not every organization can have a dedicated resource to lookup for this, but you can find security vendors that offer their services to analyze how much of your data is exposed and even monitor it.

Let's not fool ourselves, there's no such thing as the perfect defense. No matter how many security tools and regulations we have in place, all this

can only decrease the probability of an incident to happen. The idea should be to create layers of security in order to stop an attack in one of these defenses. We call these security strategy “Defense in Depth” and along with the concept of “Know yourself” even if an attack is able to trespass all these layers, we would be able to react and respond according to the threat level doing the right questions, for example:

¿Where are our most valuable assets and information? ¿How’s the shortest path from point A to point B? ¿How can I Isolate a Threat without disrupting business continuity? ¿What was the ‘Attack Vector’? ¿There was privilege escalation? ¿There are compromised accounts? ¿There was data exfiltration? ¿Where did we failed, so we can improve our security posture?

In recent years the creation of internal “Red Teams” (emulation of a cyberattack utilizing the same resources, and TTPs that an adversary would do) and “Bug Bounty” programs (testing of applications/web apps in order to find bugs) have proven to increase the maturity level of organizations enlightening vulnerabilities that wouldn't show up on a vulnerability assessment. This is another way to securely test your defenses and know your weaknesses, but also test your Incident Response, SOC or security analysts’ teams and their playbook.

So, to sum up the idea of “Know yourself”:

- Before start spending money on security tools, make a full inventory of all your assets, including a topology/network full diagram.
- Identify your most valuable data and be sure you build up your defenses around it.
- Put policies in places regarding data management and educate users to reduce the probability of human error.
- Keep hardware and software up to date, have a right schedule for testing and patching.
- Perform regular Vulnerability Assessments and eliminate known vulnerabilities.
- Monitor your information outside the fence.
- Consider to perform a “*pentest*” at least once a year.

Know the enemy

Trying to understand how an Adversary operates, wasn't something easy to get done the past, but in the last decade, different organizations worldwide, public and private, began to share all collected information about incidents, tools and TTPs on public frameworks/sites. Needless to say, the kind of positive impact this had on every organization that was not mature enough to collect and process their own Intelligence. This become a beacon for a lot of cybersecurity analysts and made new roles like "Threat Hunters", that in other words switched from only a reactive posture, to a proactive one, searching for unusual behaviors or matching patters with an adversary.

We understood that getting as much information as we can get from our adversaries, thatch us how they think and develop their attacks, how they operate and organize and the processes they go through to own an entire network. In other words: the tactics, techniques, procedures and tools they use.

Putting all this information, what we know, plus the right hypothesis, along with the circumstantial or non-circumstantial evidence to support it, we obtain Threat Intelligence. Still, this doesn’t mean that Threat Actos doesn’t change their TTPs, tools and infrastructure, but every time we make their information public, we force them to re-invent and re-create resources. Gladly for us, across Threat Actors they tend to re-use TTPs and tools, which increases our detection rates and probabilities.

Something that it’s really important and haven’t being defined yet is: ¿What is a Threat?

We can define a Threat in cybersecurity, as any Actor that has the Opportunity, Intent and the Capacity to compromise the Confidentiality, Integrity and/or Availability of our data and infrastructure in general.

The great Katie Nickels (@*likethecoins*), instructor of SANS, explained this concept pretty well on one of her webinars, but I will do my best tough.

When we analyze potential enemies and threats to our organization, we need to understand not only the capacity and resources they might have, but also their motivations. That's why today we can differentiate hacktivists, Ransomware as a service groups, from APTs. Their motivations can go from money, government espionage, corporate espionage to geopolitical, religious or belief conflicts.

Understanding an Adversary's motivations can help us to see what their final goal is, the type of organization that might be targeting, what kind of capacity they need (and might have) in order to accomplish these goals and last but not least, the needed skills.

One example of this, is the fact that today we can get information "feeds" for our machine learning security tools specially crafted to feat our industry needs and get focus on targeted attacks.

So, to sum up the idea of "Know the enemy":

- Be familiar with their Tactics, Techniques and Procedures.
- Be familiar with their tools.
- Try to analyze their Intent or motivations.
- Analyze the final goal or objectives over their actions.
- Stay up to date with their target history
- Learn from other organizations mistakes.
- Any piece of information might be useful until its proven not to.

The hundred battles

If we know ourselves and the enemy we shalt not fear the convergence point between both sides of the *clock*, the "clash" between the triangles.

This doesn't mean that knowing ourselves make our defense perfect, or that knowing my enemy make me fully prepared to defeat him. What this actually means is that understanding both sides of the equation make more plausible to know the result. Let me exemplify once again with another quote:

"He will win who, prepared himself, waits to take the enemy unprepared."

— Sun Tzu, The Art of War

Don't make yourself the "Unprepared", put the **Sand Clock** running backwards, with full awareness of your assets and infrastructure, weaknesses and strengths, and also, prepared yourself to hunt the *Enemy*, expose them, leave them with no time to fulfil or develop their plans.

As a final quote, I promise:

"Pretend to be weak, that he may grow arrogant…"

— Sun Tzu, The Art of War

They might think you aren't prepared enough, they will test your defenses and try to get as much as they can from you in order to use it against you. Even if you have a great planning, policies in place and security tools, let the "Obscurity" be your ally. Too many people think that "Security by Obscurity" is a valid security posture, but secrecy only adds an extra layer to our defenses, is not a full strategy. Nonetheless, use it in your favor.

Everything discussed so far implies a self-development over the cybersecurity maturity level, and as you can imagine, it’s a process and the ultimate goal.