The role of Intelligence in Cybersecurity

Managing today's blind spots: supply chain and human factor

2

Sally

What to find here...

The challenges of Cybersecurity in the Digital Age – 2

Intelligence Methodology – 4

The role of Intelligence in Cybersecurirty: Cyber Intelligence – 5

Introducing Digital Intelligence: Applying Intelligence to Cybersecurity blind spots – 7

Sally's Digital Security Services – 10

The challenges of Cybersecurity in the Digital Age

The security ecosystem is changing fast from heavy IT Security - almost always a step behind the malicious actors - to a changing and dynamic existence mixing the real and the digital virtual world.

Vulnerabilities appear and disappear in social networks, blogs, chats etc. and demand that security teams can address this dynamic world using the strongest human capability: Intelligence.

We are at the door of one of the more exciting challenges of modem security thinking: To include, adapt and develop the traditional information - IT and Cybersecurity process - to cover this new "digital virtual" reality outside the traditional perimeter.

Nowadays, many companies implement a management system for information security like ISO 27001, NIST or LIS (Sweden). Why? Because the implementation of a mangement system means the introduction of a systematic way of working based on the fundamentals of information security:

"SECURITY TEAMS CAN ADDRESS THIS DYNAMIC WORLD USING THE STRONGEST HUMAN CAPABILITY: INTELLIGENCE."

1. **A well defined process.**
   Inventory, classification, risk assessment, and follow-up (mitigation, controllers etc., are other words defining this)

2. **A dynamic work defined in the process elaboration,**
   where controllers are introduced to follow up and increase the security level.

This way, the security work is based on priorities that have been defined using a risk assessment process where vulnerabilities, threat scenarios and risk calculation are the core issues.

Nevertheless, when it comes to the quality of the implementation of these management systems, there are usually two blind spots: the supply chain and the human factor. Why is that?

- The introduction of a management system is mainly done by IT Engineers. However, there is a lack of security resources in the market that makes it almost impossible to manage all cyber risks.

- There is vague knowledge when it comes to supply chain risk due to the difficulty of gathering data with a satisfactory level of trust and confidence. In fact, the work with supply chain risk is usually reduced to questionnaries and forms.

- Deep knowledge of human nature seems the most preventive way for data breaches and cyber-attacks resulting from the human factor. Unfortunately, this mastery is hard to implement and requires special skills rarely found within IT Security teams.

In other words, the lack of resources in the IT and Cybersecurity market results in:

1. A lack of knowledge development when it comes to more complex risks involved in security, like the ones from supply chain and human behaviour.

   o Bad actors are clever enough to find those “non treated” vulnerabilities and exploit them.

   o We see an increase of cyber-attacks related to the supply chain.

2. The management of questionnaries and forms is a tedious task for IT-Security professionals that are used to a high level of technical complexity in their daily duties.

3. The cyber awareness programs we have seen implemented in most cases are built based on content with different pedagogical quality levels and poor follow-up activities due to insufficient measuring capabilities.

These ideas point out in one direction: Supply Chain and Human Factor vulnerabilities are not properly managed today during the implementation of information management systems or cyber security programs.

Intelligence Methodology

Most people understand Intelligence as a game for spies, secret or criminal organisations, and similar activities. Of course, many facts support this understanding: history shows the crucial role of Intelligence in significant war conflicts. Countries have been fighting battles overall, with many soldiers fighting each other. In almost all cases, the one winning the war has been using intelligence methodology to crack secrets and tactics from the other side.

There is a parallel between traditional warfare in the physical world and the cyber battle that we observe in the digital one:

- The most significant part of the battles is between IT soldiers in the trenches of the IT-security perimeter. The bad actors try to move the trenches as close to critical systems and data as possible, and the good guys try the best to defend those vital assets.

- In the same way that in the real war, the objective of the bad guys is to infiltrate networks and systems behind the trenches and open doors for the rest of their army. The good guys, meanwhile, try to move the defence line as far away from the critical assets as possible.

The role of Intelligence in any war is crucial for its development. It aims to create a significant advantage through as detailed knowledge as possible of the enemy, its tactics, and its movements. This knowledge is gathered, structured, categorised, analysed, and disseminated in understandable intelligence products that can prevent and predict enemy movements.

"THE ROLE OF INTELLIGENCE IN ANY WAR IS TO CREATE A SIGNIFICANT ADVANTAGE THROUGH AS DETAILED KNOWLEDGE AS POSSIBLE OF THE ENEMY, ITS TACTICS, AND ITS MOVEMENTS."

Intelligence complements and enriches traditional cyber security creating Digital Security programs able to address cyber security's blind spots. They do it by gathering vast amounts of digitally exposed data, structuring it, and categorising it before analysis to prevent and predict security incidents.

In the next chapter, we will focus on the role of Intelligence in Cybersecurity, considering the current cybersecurity scenario in our countries.

Keep in mind that the goal of Intelligence is not to replace anything but to help the existing security programs by enriching them with new insights that help reduce the risks before they reach the IT-Security ditches by offering a data-driven security program as automatised as possible.

The role of Intelligence in Cybersecurity: Cyber Intelligence

As we mentioned before, a parallelism between the physical world and the digital world makes it possible to talk about the role of Intelligence in both worlds. However, as we spoke of parallelism, it is essential to understand the differences between the two worlds in managing security. Those differences can be fundamental regarding to the role of Intelligence:

- In the digital world and cyber security, we apply the "assume breach" strategy saying that we already have the enemy at home, inside our trenches and behind them. On the other hand, in the real world, the goal is not to allow the enemy to breach the defensive line but to prevent the breach. Therefore, the trenches are the last line of defence and should be moved far away from the critical objects we want to protect.

- Cybersecurity efforts aim to discover the enemy as soon as possible while being breached into our systems and networks. At the same time, to build defences around information and critical objects to difficult the way in for the breached enemy. While in conventional war, we try to move our trenches forward, far away from the objectives, and we build trenches to avoid the enemy breaching our defence lines.

This parallelism between the two worlds is legit as both try to protect company assets from harmful and malicious actors that try to compromise them. However, there are also significant differences. The

strategy and tactics make Intelligence even more critical to cyber security than most people think. So let's check the data:

Regardless of the report, we will read that the human factor is still the biggest problem: Business Email Compromised, Spear-Phishing, Info-Stealers, etc., are always part of successful cyber-attack attempts.

Are you not convinced yet? Ask yourself some of the following questions:

- How are most of the successful ransomware delivered?
- Is Phishing still a significant attack vector?
- How necessary are credentials for cyber criminals?

Still not convinced? Ask us at **hello@iamsally.io**

It is a fact that investments in cyber security have been growing during the last few years by almost two digits. But it is still a fact that the number of cyber incidents and the concern for cyber security has increased even more.

The gap between the increasing activity in cyber investments and the results has increased regarding areas like human factor, supply chain etc. This hole is caused by the capabilities of bad actors to find new ways into the defence lines of companies and organisations. Those new ways are not so much related to technology attacks (brutal force etc.) but to social engineering and more complex and advanced attacks that cannot easily be managed with technology or pure IT-Security solutions. The human brain and its actions cannot be handled using IT-security technologies.

The role of cyber-Intelligence is to focus on reducing this gap by early discovering digital vulnerabilities before malicious actors, to minimise the digital risk exposure of the organisation. This way, vulnerabilities that malicious actors could use to compromise the company strategy and business goals can be eliminated or mitigated before they can exploit them.

Cyber-Intelligence is the best possible methodology for cybersecurity to move the defence line far away from the trenches of the IT-Security perimeter. It focuses on the early discovery and mitigation of digital vulnerabilities before evil actors can exploit them to get behind our security lines.

This way, companies will be able to achieve benefits that seemed to be unreachable before such as:

1. Less dependency on IT -Security Resources. Vulnerabilities can be handled before reaching the IT-Security Perimeter. (This way, IT-Security Resources can focus on what they are good at in a more sustainable way).

2. Reduction of the security gap resulting from the human factor. Therefore, Employees' training to become the first line of defence can be carried out more straightforwardly.

3.The security gap resulting from the supply chain can be managed more accurately and effectively by discovering suppliers' vulnerabilities early.

Introducing Digital Security: Applying Intelligence to Cybersecurity blind spots.

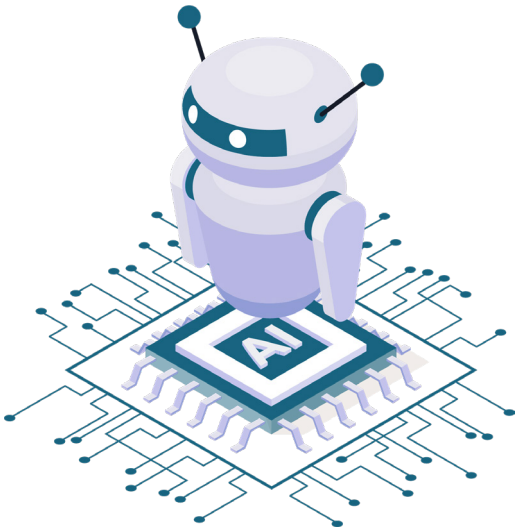
Like most things related to security and risk management, Intelligence Methodology follows a systematic process with well-defined steps and rules. Let's see some of the steps, and the types of Intelligence applied to cyber security.

1. Defining Objectives: It is essential to determine the objectives and goals, so the intelligence product results in actionable knowledge to progress in the security work.

2. Defining Assets to be protected: Similarly, as in the information security process, defining the assets to be protected is crucial. In cyber-intelligence, the assets are determined by attributes; this is the way to model them. We could call this an inventory, and as part of the inventory, we categorise the assets and their attributes by risk level.

3. Defining taxonomies: Taxonomies are a set of terms that help to structure the data gathered in the process. The data-gathering process results in a massive amount of unstructured data from all over the internet. Taxonomies will allow us to structure the data.

4. Defining Sources: it is important to define the data sources to gather as much relevant data as possible with high trust and accuracy. We can group types of Intelligence depending on the nature of the sources:



OSINT: Open-source Intelligence relates to all the sources on the open web, meaning the indexed part of the web.
DARKINT: Dark Intelligence relates to all the sources from the non-indexed web, such as deep and dark web, misconfigured databases, forums and black markets on the dark web etc.
BREACHINT: Breach Intelligence relates to the data gathered from data breaches, the small and the big ones, as they can result in a lot of vulnerabilities such as new digital identities, mail addresses or passwords, among other relevant things.
HUMANINT: Human Intelligence relates to human vulnerabilities based on the risk type, knowledge, awareness, and impact of the role of an individual in an organisation. Mostly this Intelligence is developed through conducting interviews with individuals. In Sally, we automatised this process using chatbots based on AI and ML to gather this data more effortlessly and time effectively.

5 Gathering data: Once all the above has been defined, the data gathering process can start by looking for the data across the internet. This can quickly result in a considerable amount of data that must be processed.

6 Structuring and categorising the data: Due to using taxonomies and defining assets, data can be processed by big data capabilities. At the same time, machine-learning algorithms and AI look for hidden relationships between the data documents gathered and processed to present the relevant data to the analysts.

7 Analysing the data: Human Intelligence analysts control the data presented to :
Eliminate false positives.
Work deeper into some of the data to produce intelligence products to achieve the goals defined at the beginning of the methodology.

8 Dissemination of intelligence products: The different intelligence products should be packaged in different ways and made available for the relevant people and teams in the organisation.

INTELLIGENCE METHODOLOGY FOLLOWS A SYSTEMATIC PROCESS WITH WELL-DEFINED STEPS AND RULES.

As can be seen, Intelligence is a systematic way of working following a well-defined process that needs to be reviewed from time to time or each time a new objective is included in the process.

There are, however, some essential requirements and ways of thinking that should be considered when starting an Intelligence Program:

- Data is the key to the quality of the process: The importance of the accuracy and quality of the data as well as the quantity of relevant and unique data, is key to producing high-quality actionable

Intelligence Products. The importance of this can never be underestimated in intelligence methodology. Therefore:

- The definition of the objectives and goals for the Digital Intelligence Process is vital to determine the kind of data that must be gathered.

- The definition of the proper taxonomies for the relevant goals will increase the equality of the products.

- Access to privilege and relevant data is as well a critical point. It is mandatory to check the kind of data the solutions have access to. (The knowledge about relevant sources must be secured from the very beginning).

- Structuring and categorising the data in an automatised way will secure the production time of the intelligence products and avoid much noise generated by insufficient data processing. Big Data capabilities, Machine Learning and AI should be implemented in the solution to short time to production and secure quality.

- Consider is the ability to find good analysts that can give the last intelligence touch to the product adding Human Intelligence to discard false positives and point out areas to dive deeper into starting investigations.

- In the implementation process and as a direct consequence of the objectives and goals, **disseminating the product inside the organisation is crucial** to take advantage of the intelligence products.

A Digital Intelligence Security Program is a systematic way of working with a data-driven security approach to reduce the risk exposure of the company assets in the digital world for early prevention of security incidents before they reach the organisation's perimeter.

In other words, we could say that Digital Intelligence Security Program is a possible implementation of the "Prevent Breach" strategy that complements the traditional "Assume Breach".

Sally's Digital Security Services

Sally tries to make Intelligence available to all kinds of companies regardless of their size. We do so by packaging intelligence products easily and affordably; affordable for us means not only economically but adapted to the company's different departments so they can use the actionable Intelligence without any previous knowledge.

Sally offers actionable data-driven intelligence insights for different levels of security of the company aiming to introduce all the benefits of Intelligence without investing in tools, people, and data upfront. It is a first step into data-driven digital security and an easy and affordable way to enjoy all its benefits.

We at Sally have modelled the threat landscape outside the IT-Security Intelligence and used Intelligence and privilege data to create automated digital rounds for surveillance from outside of the IT-Security Perimeter (outside surface), supply chain, digital exposure, and human factor. In other words, we look for human, technical, digital and supplier vulnerabilities to manage digital security and mitigate digital risks.

Sally

YOUR SECURITY ALLY

Contact us

hello@iamsally.io

iamsally.io

iamsally_safety

I am Sally