Cyber Counterintelligence: When Defense Alone is No Longer Sufficient

SARA JELEN - author

Sara believes the human element is often at the core of all cybersecurity issues. It's this perspective that brings a refreshing voice to the SecurityTrails team. Her ability to bridge cognitive/social motivators and how they impact the cybersecurity industry is always enlightening.

"The best defense is good offense" is a saying that can be applied to many fields: military, games, business… and **cybersecurity**. However, the standard 'defense-only' approach many organizations have been taking is simply not sufficient for dealing with the current threat landscape. And just as intelligence services keep an eye on terrorists to stop them before they attack, organizations should move towards **adopting the offensive approach to protect their infrastructure and systems**.

Contents:

In today's unpredictable cyberspace, cybercriminals are constantly developing more and more advanced techniques and technologies. This means that traditional defensive cybersecurity solutions, reactive once the attack takes place and easily evaded, are simply ineffective on their own.

Organizations need to focus on crafting more innovative approaches to safeguard their environment, one of which can be employment of a purple team. Getting into the mind of the attacker and adopting offensive techniques will go further than the defense-only approach to proactively mitigate cyber risks and uncover advanced threats in their network.

While cyber counterintelligence (CCI) has been used by state actors for some time now, its importance to other, non-state organizations has been recognized. Both large and small organizations are increasingly targeted by cybercriminals aiming to steal their critical information, with attackers ranging from competitor companies, organized cybercrime groups and even a country's government. For this reason, **cyber counterintelligence presents itself as an innovative approach that unifies active-passive and offensive-defensive approaches to fortify an organization's infrastructure and protect against attacks**.

Today we'll explore the concept and strategy behind cyber counterintelligence and examine its advantages and disadvantages.

What is cyber counterintelligence?

Cyber counterintelligence (CCI) is officially defined as:

"Measures to identify, penetrate, or neutralize foreign operations that use cyber means as the primary tradecraft methodology, as well as foreign intelligence service collection efforts that use traditional methods to gauge cyber capabilities and intentions."

We can also define CCI as efforts made by an organization to prevent malicious actors, competitor intelligence advances, nation states or criminal organizations from collecting sensitive information about them, such as intelligence data, for example IP intelligence. Although the objective of cyber counterintelligence is defensive, the methods are essentially offensive. In other words, in order for cyber counterintelligence to be effective, it needs to be both offensive and defensive.

Various techniques are employed to implement the defensive and offensive operations of cyber counterintelligence. The techniques themselves are difficult to separate into categories of "defense" or 'offense" however, so the unity of both approaches is needed.

Let's find out more about these two approaches, and how they look in the CCI process.

The cyber counterintelligence process

The purpose of CCI is to identify, deter, degrade, neutralise, and protect against adversary intelligence activities. This is done through a process that utilizes both passive and active counterintelligence approaches, with the aim of protecting organizations, so let's delve deeper into both to better understand the entire CCI process.

Defensive cyber counterintelligence

Defensive cyber counterintelligence are actions taken to identify and deflect adversaries **before they attack**. The purpose of defensive CCI is to protect the organization against vulnerabilities and internal and external threats. In addition to traditional security measures such as firewalls, IDS's, anti-virus solutions and

encryption, **defensive CCI is also comprised of penetration testing, vulnerability assessment and management, threat intelligence, threat hunting and more**.

Penetration testing

Engaging a red team to perform their assessment and pen testing to detect vulnerabilities, as well as test an organization's network and systems using attacker tactics, will provide the organization with insight into possible attack vectors, network and system weaknesses and their attack surface. This will prepare the organization for better detection and more effective response to any possible threats.

Red team assessments and penetration testing would be considered an active defensive cyber counterintelligence.

Vulnerability assessment

Once possible network threats and vulnerabilities have been identified, often with the use of vulnerability scanning tools, the next step is to perform a vulnerability assessment, which is essentially a more passive defensive CCI. This is done by defining, classifying, and most importantly, prioritizing vulnerabilities found in the systems and network infrastructures. This step informs the organization toward being better able to understand threats and, in turn, react to them quickly and effectively.

Threat intelligence

Predicting future attacks before they even reach your network helps organizations prioritize responses as well as speed up the response time, which provides better security posture. Of great use here is threat intelligence, which is defined as collecting and analyzing data about indicators of past, current and future cyber threats. This enables an organization to take the actions needed to protect their environment—with the keyword being "analysis."

Threat hunting

Once we've performed analysis, which is a more passive action, we come to threat hunting, an active defensive CCI operation. Threat hunting is the act of proactively searching for cyber threats in an organization's network. It involves detecting and isolating the more advanced threats that might have evaded traditional endpoint security measures.

Offensive cyber counterintelligence

Offensive CCI is considered active interaction with the attackers. This includes collecting information about their intelligence process, techniques, capabilities and even deceiving them by presenting false information and leaving “open” access points that trick them into thinking they have accessed confidential information. All of this takes place while the organization monitors the attackers, again, collecting information that will support effective measures against them. This can be done with the use of honeypots, honeynets, false flags and sockpuppets.

The purpose of offensive cyber counterintelligence is to manipulate the intelligence operations of the attacks through deception, disinformation and exploitation.

Honeypots

Honeypots are systems or applications created to attract attackers who are trying to attack computer networks. They are, essentially, isolated trap systems that are strictly monitored by the organization.

Honeypots are specifically designed to be vulnerable, to easily attract malicious actors who will try to exploit them. Once an attacker falls into this trap system, system administrators can then gather valuable intelligence data on the attacker, including their techniques. They may even possibly identify the attacker.

Sockpuppets

Sockpuppets are social and online fabricated personas that have a credible social history and appear legitimate. They’re used to interact online, to collect information about potential adversary operations and their capabilities. OSINTgoes hand in hand with HUMINT (human intelligence), and sockpuppets are a great way to gather that type of information.

Truly effective sockpuppets can potentially infiltrate an adversary’s entire operation and even create double-agents to learn more about the adversary intelligence operations who are targeting them.

Disadvantages of cyber counterintelligence

While the importance and advantages of cyber counterintelligence are clearly visible in the complex and multi-layered approach of passive-active and defensive-offensive techniques and actions, there are still reasons why CCI isn't widely utilized by organizations.

Cost

The broad and often complex operations needed to perform cyber counterintelligence call for a team of experts, assembled for and dedicated to their shared goals. This of course means there is a significant, sometimes prohibitive, cost in question. The good news is that the need for CCI is mostly noticeable in larger organizations with rivals and other corporate entities with an interest in gathering intelligence on them for attacks.

While larger-scale organizations might not wrestle with as many budgeting obstacles as smaller concerns, the pricey nature of CCI still can't be overlooked.

Legality

The notion of engaging in cyber counterintelligence shouldn't be taken lightly. Many of the actions it requires can dance on the line of legality—and even sway the organization into breaking the law to protect their infrastructure. This can result in a flurry of legal problems, so the process of understanding and planning the entire operation is crucial. Every possible scenario needs to be covered.

Failure

As with anything in cybersecurity, failure is always a possibility. Although cyber counterintelligence might sound like the perfect solution for keeping organizations safe against adversary intelligence operations, you can never be 100% secure. Combined with the potential for legal issues and the high cost of implementing CCI in an organization's cybersecurity measures, it's easy to see why CCI isn't more widely adopted by non-state organizations.

Conclusion

Organizations are under the constant threat of adversary intelligence and cyber espionage operations, making the need for cyber counterintelligence in the current threat landscape significant. It's also important to understand the multi-layered and multi-disciplinary approach CCI requires to be fully effective in thwarting future attacks by rivals, corporate entities, organized cybercrime groups or countries' governments.

The unity of active and passive as well as defensive and offensive actions plays an important role in employing CCI. This multi-pronged approach provides organizations with a better security posture in the face of ever-evolving adversaries and their tactics.

"Attack is the secret of defense; defense is the planning of an attack."

— Sun Tzu, The Art of War
