Carbon Black.

Cognitions of a Cybercriminal

Introducing the Cognitive Attack Loop and the 3 Phases of Cybercriminal Behavior

JULY 2019

Dear CISOs,

We have a fundamental saying at Carbon Black: “Cybersecurity is all about the data.”

I love this saying. In understanding the data, we can better understand behaviors. And, in better understanding behaviors, we can better understand attackers.

Much like a detective in the physical world pieces together information to solve a robbery, Carbon Black instantly pieces together all of the relevant endpoint data to better understand how criminals behave.

When it comes to cybercriminal behaviors, the Lockheed Martin Cyber Kill Chain® has been the de facto standard for years. I believe we should be looking at this model with a new lens. Attackers have evolved dramatically in recent years by using fileless attacks, lateral movement, counter incident response and island hopping in attacks. Consequently, we must be measuring success in how well we can disrupt these behaviors.

To that end, I am proposing what we’re calling the “Cognitive Attack Loop” —a three-step cycle that continues to repeat and evolve. Attackers are dynamic and constantly evolving. It’s no longer helpful to approach cybersecurity linearly. As this paper will discuss, cognitions and context help reveal intent. Understanding the root cause of attacks and the way attackers think is paramount to this.

To be effective at cybersecurity, we need to get inside the minds of cybercriminals and understand the motivations driving their behaviors. Attackers have “tells,” much like poker players. These “tells” often appear in the data. Defenders can exploit these tells and gain the advantage by understanding the data.

Thank you for reading this paper and for joining me here as we delve into the cognitions that govern cybercriminal behaviors.

And, if you’re interested in hearing more, check out the recent webinar we did on the topic, or visit Carbon Black’s Howler Hub!

Tom Kellermann

Tom “TK” Kellermann
CHIEF CYBERSECURITY OFFICER | CARBON BLACK

Evolution in Cybercrime Behaviors

Attackers are getting better at moving around inside systems without being detected. According to the latest Verizon Data Breach Investigations Report (DBIR), 68% of attacks go undetected for months or more. Elite cybercriminals know how to subvert traditional cybersecurity techniques because of the industry's historical overreliance on legacy antivirus (AV) and Indicators of Compromise (IOCs).

To remain undetected by legacy antivirus, cybercriminals are increasingly using fileless and living-off-the-land attacks, versus commodity malware. According to the DBIR, only 28% of attacks use malware (down from 51% in 2017). This is congruent to Carbon Black's own research, as well as research from some of Carbon Black's partners, like Red Canary, which found PowerShell-based attacks to be the most prevalent in its 2019 Threat Detection Report.

Attack evolution does not stop there, though. Today, 70% of all attacks now involve attempts at lateral movement and 51% leverage island hopping, according to Carbon Black's 2019 Global Threat Report.

This means that security teams need to be evaluating the security posture of all organizations in their information supply chain—traditional security tools can't be relied on. Cybersecurity needs to use predictive behavior analysis to achieve true visibility.

Carbon Black's Global Incident Response Threat Report showed that 56% of incident response (IR) professionals see counter incident response techniques being used during engagements and another 70% witnessed evasion tactics.

Furthermore, if the attacker knows they've been caught, many will execute a destructive script and destroy as much of your data as possible on the way out. Carbon Black's research found that 31% of targeted victims now experience destructive attacks.

Security roles now involve hunting and suppressing cybercriminals without them knowing. We need to detect, divert, contain and hunt in a clandestine fashion. This is critical to decreasing dwell time and limiting damage.

ONLY 28%

OF ATTACKS INCLUDED MALWARE

56%

OF IR PROS SEE COUNTER-INCIDENT RESPONSE

70%

OF ATTACKS INVOLVE LATERAL MOVEMENT

70%

OF IR PROS WITNESS EVASION TACTICS

51%

OF ATTACKS LEVERAGE ISLAND HOPPING

31%

OF ATTACKS ARE DESTRUCTIVE

To Combat Evolving Attack Behaviors, the Security Paradigm Must Change

Meeting Cybercriminals at the Poker Table

We used to think of cybersecurity like physical security. If you block all the entryways, you're safe. But in cybersecurity today, there is no way to prevent 100 percent of attacks 100 percent of the time. Finding threats is now about meeting attackers head-on in your systems and making decisions based on their behavior. You are essentially playing a poker game, and understanding the "tells" of your attacker will allow you to defend your chips and walk away victorious.

Much like at the poker table, attackers make decisions and change their strategy during play. Your security team needs to play the players—using data to make the best decision for each hand. You should continually be asking yourself, "How can I best manage my risk?" while gathering the proper information to help you make decisions. You don't want to take a big risk without data. Supplying your security team with better visibility results in better decisions and helps them hold a strong position at the table.

> **"The dark web has become an arms bazaar of attack tools which are being deployed by a multiplicity of actors, creating a virtual free-fire zone. Now that elite cyber weapons are available to all, CISOs need to be worried about the impact of this trickle down economy."**
>
> – **Rick McElroy** | Principal Security Strategist | Carbon Black

PLAYER

Nation-State Actors

TARGET

Governments and businesses running critical infrastructure like power grids.

WHY THEY ARE PLAYING

Steal sensitive information, disrupt enemy capabilities or create international incidents.

HOW THEY GAIN CHIPS

Sophisticated cyberattacks where the adversary often works directly or indirectly for their government and utilizes highly advanced cyberattacks against targets.

MOTIVATION

Putting their nation in a better position against supposed enemies.

STAKES // EXTREMELY HIGH

PLAYER

Cybercrime as a Business

TARGET

Companies with customer data (particularly financial data) or valuable IP.

WHY THEY ARE PLAYING

Steal sensitive information that can be sold or directly steal money. Proceeds may be used to fund other criminal activities, hence the nickname criminal "ring."

HOW THEY GAIN CHIPS

Infiltrate networks, often through a less secure partner, and retrieve the sensitive data.

MOTIVATION

Money.

STAKES // HIGH

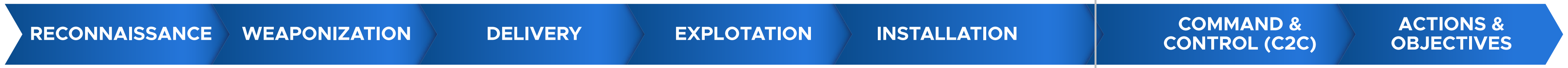
The Need for an Updated Kill Chain

Several years ago, Lockheed Martin introduced the “Cyber Kill Chain” to the community. According to Lockheed Martin, “the model identifies what the adversaries must complete in order to achieve their objective.”

Even if you’re relatively new to cybersecurity, it’s likely you’ve heard of (or even referenced) the Lockheed Martin Kill Chain at some point during your career. This kill chain has been a helpful, albeit sometimes criticized, tool that focuses highly on prevention-heavy security strategies:

Theoretically, if you can disrupt attacker behavior as soon as possible in the Kill Chain, you not only drive up the cost of the next attack but also enable teams to begin to stack defenses along the chain, which offers a better chance of stopping the attack. One disruption in the chain breaks all the downstream steps.

The Kill Chain did an excellent job describing the distinct phases of attacks and served as a good guide for defenders. However, it didn’t describe how or why the attackers were performing attacks this way.


RECONNAISSANCE
WEAPONIZATION
DELIVERY
EXPLOTATION
INSTALLATION
COMMAND & CONTROL (C2C)
ACTIONS & OBJECTIVES

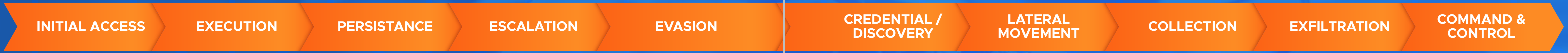
Enter MITRE ATT&CK™

In 2018, MITRE introduced a game-changing framework for defenders in “ATT&CK,” which became the equivalent of being able to see your opponents’ cards at the poker table.

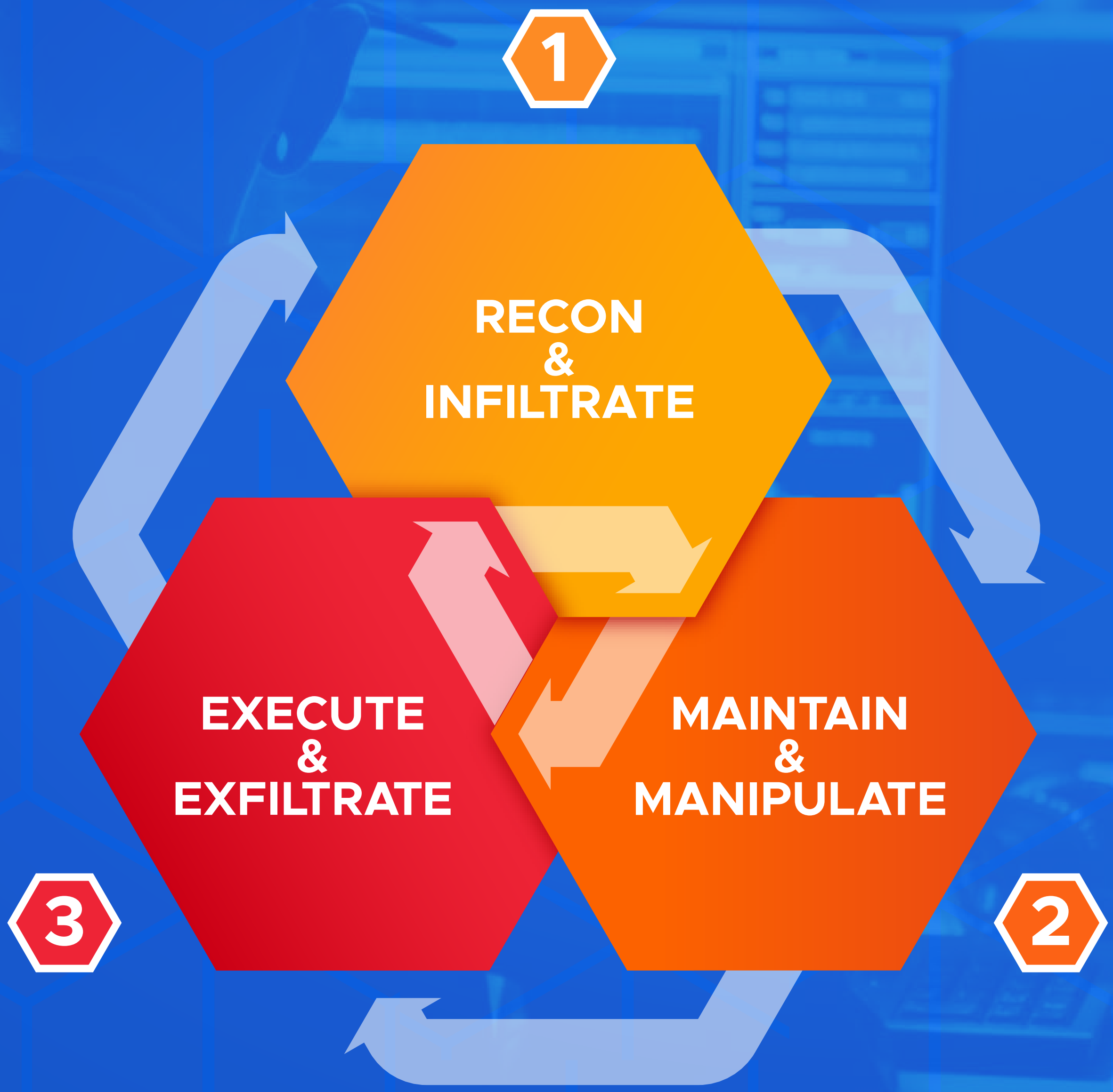
MITRE ATT&CK defined not only the phases of attacks but also showed how the opponent would behave. In our opinion, MITRE ATT&CK was an earnest effort to make everyone better. They later doubled down on the efforts with some unbiased testing of leading security vendors, including Carbon Black. It will be interesting to see how we as a community leverage this framework for the long term. To continue the poker analogy, MITRE ATT&CK is basically the equivalent of Doyle Brunson’s “Super System: A Course in Power Poker,” which made a lasting impact on the game.

The evolution from the Lockheed Martin Kill Chain to MITRE ATT&CK changed our style of play of cybersecurity.

There has been an explosion in the talent behind cyberattacks. The skills aren’t in a few number of hands anymore. For a while in poker, you saw the same handful of people win the World Series of Poker over and over again. Then the game changed due to an influx of talent from online poker, where anyone at home could develop new strategies and techniques and new players could see an infinite number of hands at once. In one year, players could rack up the experience it would generally take years or decades to develop. The cloud changed poker and it’s changed security too.


INITIAL ACCESS
EXECUTION
PERSISTANCE
ESCALATION
EVASION
CREDENTIAL / DISCOVERY
LATERAL MOVEMENT
COLLECTION
EXFILTRATION
COMMAND & CONTROL

Introducing the Cognitive Attack Loop and Its 3 Phases



The Data Behind Cybercriminal Behavior

Carbon Black has architected its security solutions to focus on monitoring cybercriminal behavior. The hypothesis from the start was that the more insight we have into cybercriminal behavior, the more effective the technology would be in recognizing suspicious activity and hunting it successfully.

We conduct behavioral threat research to discover novel patterns used by attackers. These patterns stretch across the entire scope of the kill chain, transcending any individual attack and allowing us to provide protection against a broader set of threats (malware, fileless, living-off-the-land) without relying on specific pre-discovered IOCs, like hashes or command and control (C2) capabilities that have traditionally been used to detect threats. Our research involves identifying threat patterns and building models to detect and prevent these threats on the fly, keeping false positives as low as possible.

We collect eight to 15 terabytes of data per day from around the globe. Furthermore, the top incident response firms all over the world use our technology in at least one breach investigation per day, on average, in order to identify and contain cybercriminals. This means we have amassed a lot of data on cybercriminal behavior. After studying this data, we've found distinctive patterns in that behavior. Our goal is to help you better understand what you're up against and how to defend against it.

The Cognitive Attack Loop

From this research, we've identified three phases in cybercriminal behavior:

1. Recon & Infiltrate
2. Maintain & Manipulate
3. Execute & Exfiltrate

These phases are represented as a cycle because there are important subtleties in how today's cybercriminals are operating.

> **"Executives today are misinformed about who cybercriminals are because movies and shows propagate the sinister, hoodie-wearing image. They need to be educated about the motivations and behaviors of today's cybercriminals in order to make better decisions on where to invest in security."**
>
> – **Paul Drapeau** | Enterprise Security Architect | Carbon Black

PHASE 01: Recon & Infiltrate

In the initial phase of cybercriminal behavior, the attacker is preparing their operation. We call this the "Recon & Infiltrate" phase. This can include selection of the target, determining the best means to gain access to the target and actually gaining that access. In some cases, the threat actor may have a specific target and toolset in mind, but they may also be very flexible in selecting targets of opportunity or tuning specific attacks to a given target.

This phase is also common in lateral movement and island hopping attacks where an attacker is leveraging execution, command and control already achieved to continue their cycle onto a new target system or organization.

THE FIRST PHASE OF THE COGNITIVE ATTACK LOOP

Breaking Down Recon & Infiltrate Behaviors

- **GATHER INTEL:** Cybercriminals select a target and learn relevant information such as vulnerabilities, network information, third-party interactions, employees, etc. The more they know, the more successful they feel they will be. *In poker terms, they are choosing a table to target and observing opponents to look for tells.*
- **EXPLOITATION:** At this point, a cybercriminal will deliver a payload designed to get initial access to the target via an identified or discovered vulnerability. *They are raising the stakes at the table to see what the response is.*
- **SOCIAL ENGINEERING:** This involves attacking the human element of the target organization via email, phone, physical or other electronic means. This can include watering-hole attacks, phishing or spear phishing. *The cybercriminal is making outlandish bluffs or faking a tell to throw you off your game and make you lose focus.*
- **DELIVERY:** Once access is achieved, the cybercriminal will deploy the initial stages of an attack into an environment. This may be the first payload resulting from an exploit or a social engineering document. *At the poker table, they won a hand, learned more about your responses and took some chips.*

DEFENDER ROLE DURING: **Recon & Infiltrate**

It is very difficult for most defenders to detect attacks during this phase. Many of these behaviors are normal events defenders face and are not seen as part of a larger threat. The only way to recognize these behaviors for what they are is to increase visibility with solutions that can monitor behaviors and look for patterns to indicate that recon and infiltration is happening.

PHASE 02: Maintain & Manipulate

During the second phase of criminal attack, "Maintain & Manipulate," attackers are already "in your house" and you need to get them out. Paramount to your success is understanding how they have "maintained a foothold" in your environment. In this phase, the attacker is using their initial access to continue to improve their position to move forward with their goals. Often, to achieve whatever ends the attacker has in mind, they need additional access levels or to circumvent existing controls.

THE SECOND PHASE OF THE COGNITIVE ATTACK LOOP

Breaking Down Maintain & Manipulate Behaviors

- **EXECUTION:** After the initial payload is delivered the attacker expands their command and control capabilities with additional tools or modules. *At the poker table this would equate to the attacker shifting their attention to other players in order to gain chips to later use against you.*
- **PRIVILEGE:** Typically, attackers need to elevate privileges or permissions on the target system or network. Techniques associated with this tactic include further exploitation to gain system or administrator permissions, stealing credentials to facilitate things like lateral movement or escalation. *During the poker game, attackers won't hesitate to exploit the tells of other players in order to gain chips.*
- **PERSISTENCE:** At attacker normally requires continued access to the target as well as their toolsets installed in order to maintain access across reboots or in the face of defensive capabilities. These tools allow the attacker to restart and reestablish, if necessary. *They are now positioned with a high stack of chips and are prepared to stay in the game for a long time.*
- **EVASION:** Attackers respond to defender behaviors and defensive controls by adapting their behaviors to continue their mission in the face of such obstacles. Evasion behaviors may involve turning off security controls, adapting command and control protocols to blend into typical network traffic or hiding tools on the file system. *Now you're active in the game and called the attacker's bluff. It worked for one hand, but they change up their strategy the very next hand.*
- **COMMUNICATION:** To continue their mission attackers establish command and control (C2) capabilities. This network-based communication allows attackers to interact with the compromised system and introduce new tools in real time. *In real life, the cards you get are the cards you're stuck with. But imagine if your opponent could "download" a better hand on demand. Not fair, right? Unfortunately, that's exactly what adversaries are doing today.*

DEFENDER ROLE DURING: **Maintain & Manipulate**

During this phase defenders need to be engaging. That means that telemetry is needed to begin to push adversaries out. But there's a catch. Attackers are now excellent at evasion and ready to execute destructive scripts in the next phase. That requires hunting them in a clandestine fashion so the attacker isn't alerted to your efforts and strategy.

PHASE 03: Execute & Exfiltrate

In the "Execute & Exfiltrate" phase, the attacker is executing on their end goals. This may be gaining access to one system in a network where the end goal is moving laterally. Alternatively, it may be accessing the final target system where the attacker is looking to compromise the integrity, confidentiality or availability of information. Or, it may just be establishing access for the attacker to leapfrog/island hop into another external system or transfer to a third party. Remember, island hopping is on the rise and your worst case scenario is if your network, website or mail server is used to leverage attacks against your constituency. The implicit trust in your brand will be used against your customers.

THE THIRD PHASE OF THE COGNITIVE ATTACK LOOP

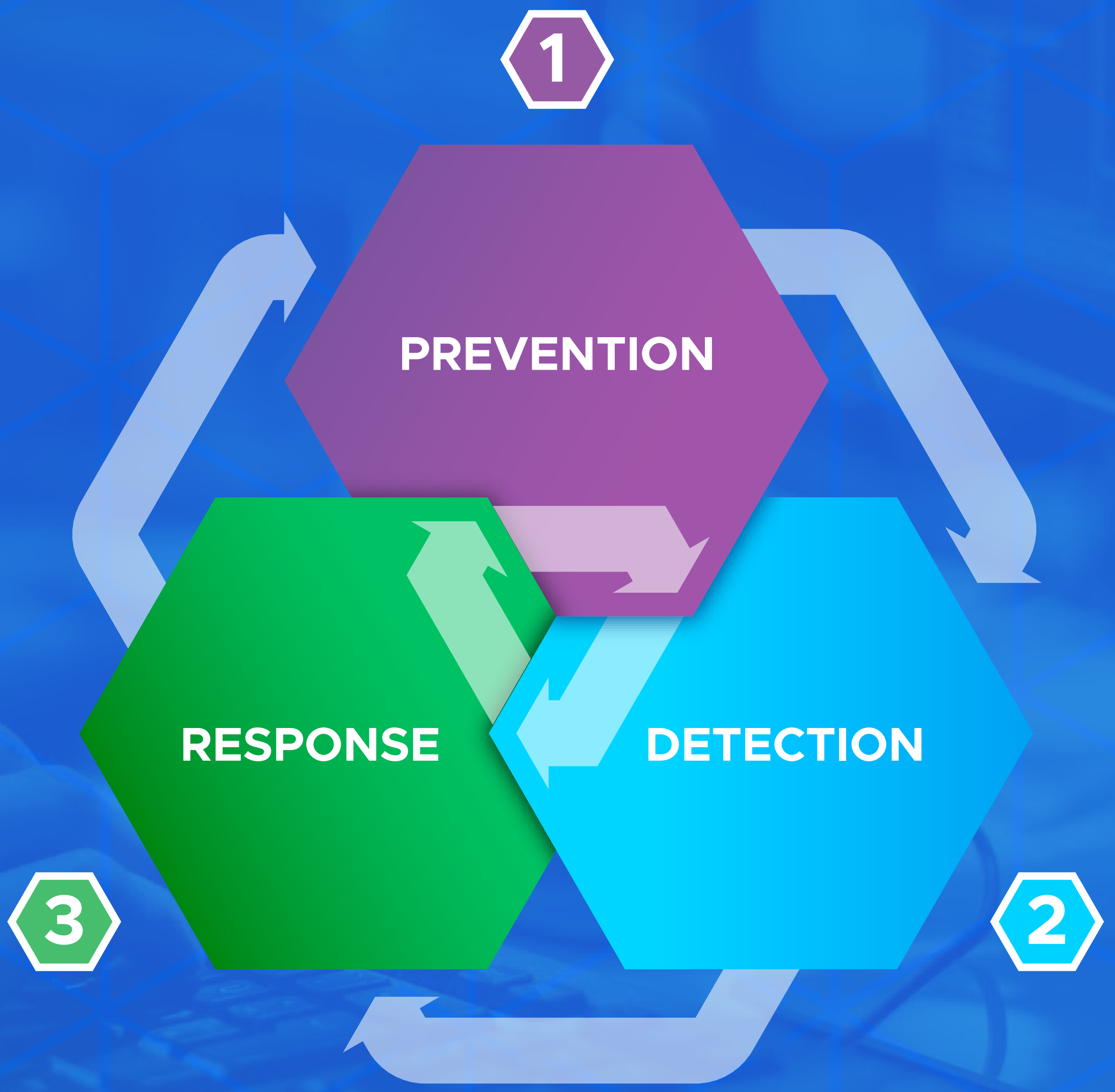
Breaking Down Execute & Exfiltrate Behaviors

- **CAPTURE:** Attackers need to collect critical information as part of many operations. This may include file access, keystroke logging, screenshotting, camera or microphone access or any manner of data extracted from the target system. In many ways, this phase is returning us back to the start of the cycle and the recon phase. *At the poker table they are intently studying you for tells and weaknesses in your strategy to exploit.*
- **EXFILTRATION:** Attackers commonly move data out of the target environment for purposes of profit, espionage or offline analysis. Data is transferred from the target system/network to the attacker's C2 infrastructure via network or physical means. *Basically, they are slowly, yet consistently, taking your chips.*
- **DESTRUCTION:** Some attacks involve destruction of information for profit or disrupting the target's operations. Examples include ransomware, wipers, etc. *If they recognize your bluff, they will call you on it.*
- **DISINFORMATION:** All manner of false actions taken by an attacker to conceal their true intentions or the nature and magnitude of the operation. Typically, disinformation includes anti-forensics such as log deletion or manipulation, or destruction tactics as a secondary cover. *Even after winning a big hand, the attacker will bow out of future hands or fake tells to throw you off your preconceived notions of their behaviors.*

DEFENDER ROLE DURING: **Execute & Exfiltrate**

This phase of the attack is where it is most important for defenders to contain and eliminate the threat. If the goal of the previous phase was to learn the attacker's tell, the goal now is to get them to give up their chips. That means you need automated response and remediation tools to act quickly upon data capture, as well as strong behavioral prevention rules to stop exfiltration or destruction.

Cognitive Defense Loop



Attack cycles don't end so why should your defenses. We need to look more broadly at our own strategies and adjust our game play to be successful during this new style of play. We need to treat our prevention, detection and response as a cycle that feeds each other and makes each other stronger over time and as a result of each attack. Layering the combination of behaviors and tactics, techniques and procedures (TTPs) together will allow you to weave the right strategy of people, process and technology to tip the odds in your favor.

Poker is just as much about playing the player as it is playing the hand you've been dealt. Players have tells. So do attackers. Players get tired. So do attackers. Players get frustrated and go "on tilt." So do attackers. You have to put yourself in a position to dictate the way others play when they are at your table. At your table, you should know how the players play and how understanding that cognition will allow you to use that against them.

A new strategy should account for not only the current threatscape but also take into consideration the past to better understand the future landscape. Having the ability at scale to store, sort and make use of this data to understand the most likely next attack vector is critical.

Prevention shouldn't happen alone, it should be constantly fed and tuned by new information. The same holds true for detection and response. These functions need to be considered paramount to the success of any security program. You need a stack built around that premise. You need to combine behaviors and TTPs (not IOCs).

If anything, a more cognitive approach to defense will allow for a better understanding of what's normal inside your environment. In poker terms, when does your opponent normally re-raise? When are they bluffing or when do they have the best hand?

This approach allows for greater precision in remediation steps as well as drives positive security changes on a more regular basis. This also allows for the most chances of disrupting an attack. We covered why the kill chains are important and why interrupting each phase makes the attacker work harder at each step or causes the entire chain to break. Now we need to apply that to a never-before-seen scale and a changing game. The "Cognitive Defense Loop" is powered by the behaviors of attackers and enabled by TTPs. It's time we combine prevention, detection and response into one to gain an upper hand at this more sophisticated game.

My Advice to CISOs

After reading this paper, I hope that CISOs feel encouraged that there is a way to win at the cybersecurity poker table. It just takes a shift in security investments and careful thinking about weaving the behavioral aspect of cybercriminal cognitions into your security processes. Here are some steps you can take to gain better visibility into cybercriminal behavior within your systems.

7 Action Items for CISOs

1. □ **EVALUATE YOUR CURRENT SECURITY STACK**
   Determine where the gaps are in your tech stack in obtaining behavioral data, enabling automation and orchestration, allowing customized watchlists and pattern recognition, and assisting the hunt with deception technologies. Create a plan to begin to fill these gaps.

2. □ **SCRIMMAGE IN CYBERSPACE**
   Conduct a penetration test or compromise assessment from inside out to identify all viable attack paths that an adversary can use to move laterally.

3. □ **SHIFT AUTHORITIES AND BUDGETS**
   Once you have a plan to fill the gaps, you'll need to get executive buy-in to make changes. Utilize this paper and the simple poker analogy to help them understand the need. Then shift investments toward tools to recognize behavior in response to the nature of today's threats.

4. □ **SIMPLIFY OPERATIONS**
   Once you've begun monitoring behaviors, use behavioral threat patterns to orchestrate and automate collaboration, remediation and other operational tasks across the entire security stack.

5. □ **IMPROVE PROTECTION AND RESPONSE**
   Decrease IR time by setting up appropriate prevention controls, using data to get to root causes of entire classes of attacks, and zeroing in on incidents with all the information at your fingertips.

6. □ **CONTINUOUS LEARNING**
   Cybercriminals continue to evolve. Make sure your team is learning about new behaviors by connecting with the 20,000 cybersecurity pros in the Carbon Black User Exchange and by proactively exploring the data in your own environment. Additionally, you and your team leaders will want to follow the threat research from Carbon Black to stay on top of the latest threats and cybercriminal trends.

7. □ **SEE THE OTHER SIDE OF THINGS**
   Empower your red blue to see the blue team side of attacks and vice versa. It's critical to see the landscape from multiple points of view to gain a full perspective. Teams can learn a lot from looking at a problem through multiple lenses.

Carbon Black.

ABOUT CARBON BLACK

Carbon Black (CBLK) is a leader in cloud-native endpoint protection dedicated to keeping the world safe from cyberattacks. The CB Predictive Security Cloud® (PSC) consolidates endpoint security and IT operations into an endpoint protection platform (EPP) that prevents advanced threats, provides actionable insight and enables businesses of all sizes to simplify operations. By analyzing billions of security events per day across the globe, Carbon Black has key insights into attackers' behaviors, enabling customers to detect, respond to and stop emerging attacks.

More than 5,300 global customers, including 35 of the Fortune 100, trust Carbon Black to protect their organizations from cyberattacks. The company's partner ecosystem features more than 500 MSSPs, VARs, distributors and technology integrations, as well as many of the world's leading IR firms, who use Carbon Black's technology in more than 500 breach investigations per year.

Carbon Black, CB Predictive Security Cloud and CB LiveOps are registered trademarks or trademarks of Carbon Black, Inc. in the United States and/or other jurisdictions.

1100 WINTER STREET, WALTHAM, MA 02451, USA • P 617.393.7400 • F 617.393.7499 • WWW.CARBONBLACK.COM