Carbon Black.

GUIDE

Building a High-Speed SOC

INTRODUCTION

WHERE HAS THE TIME GONE?

With breaches today often going undetected for months or years, many organizations must now accept the very real possibility that intruders have already compromised their systems, regardless of the organization’s security posture. Today, compromises are measured in minutes and the speed of response is measured in days. Enterprises the world over are realizing that to close the gap, they need to evolve their security operations from being a largely reactive unit (waiting for alerts that indicate a threat) to being proactively on the hunt for new attacks that have evaded detection.

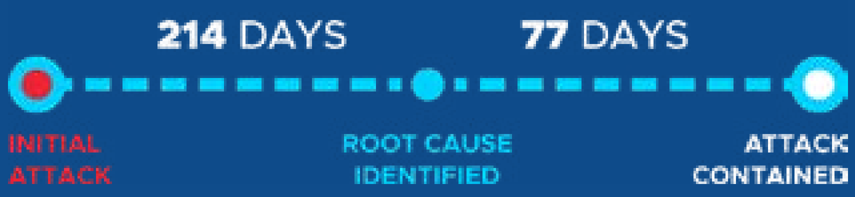
SPEED STOPS BREACHES

When an incident does occur, the speed of your response will dictate the extent to which you can minimize the impact. In the case of a malicious attack, it takes on average over 7 months to identify a breach, and nearly two and a half additional months to contain the incident. Every second counts, and while the clock is ticking, the cost of the breach is rapidly increasing as well. Breaches that take over 30 days to contain cost companies an extra $1 million, and depending on the severity, it can cost even more. Minimizing dwell time is the name of the game; the faster you can identify root cause, the faster you can remediate.

SPEED STARTS NOW

A highly efficient security operations center (SOC) enables its skilled defenders to harness both advanced automation and human insight to combat the ubiquitous threat of cybercrime. The time to transform your SOC into an intelligence-driven operation that can hunt for zero-day threats is not after an incident when you realize you lack the information for proper forensic analysis. Put your SOC and your team in a position to succeed today by taking inventory of just how effective and well-integrated your security stack is in the face of modern sophisticated cyberattacks.

On average, it takes over **9 months** to disrupt a malicious attack:



People & Process Problems

GOOD HELP IS HARD TO FIND

Building a high-performing SOC can be challenging with a scarcity of skilled defenders. In a recent survey, 46% of organizations said they noticed a “problematic shortage” of cybersecurity skills, and 87% claimed that it is difficult to recruit and hire new cybersecurity talent. While it is becoming increasingly clear that advanced technical skills are in demand, many organizations also understand that every environment is different. In order for an analyst to properly defend your infrastructure, there is a great deal of on-the-job learning that must take place, both in regards to the people and assets being protected, as well as all the tools being used to protect them. This does not necessarily mean that new analysts are all unqualified, but rather there is an opportunity for them to learn as your SOC grows.

46%

OF ORGANIZATIONS SAID THEY NOTICED A “**PROBLEMATIC SHORTAGE**” OF CYBERSECURITY SKILLS

As roles change and the hierarchy of the SOC evolves, the most basic triage falls on entry-level analysts who spend most of their days minding a steady flow of alerts. If the analyst is lucky, the alerting has been tuned and the tools he or she is using minimize false positives that muddy the waters of threat prioritization. However, there is a strong chance that analyst’s situation resembles the **37% of organizations who cite keeping up with the volume of alerts as one of the biggest incident response challenges.** The analyst is forced to rely on their limited experience to guess at how serious each alert is, but to keep up with the sheer volume, these decisions must be made quickly. Without extensive experience actually responding to investigations, your first line of defense is this overwhelmed analyst.

87%

OF ORGANIZATIONS CLAIMED THAT IT IS DIFFICULT TO RECRUIT AND HIRE NEW CYBERSECURITY TALENT

TIERING UP

Lacking sufficient context to address any worrisome alerts, a tier one analyst will pass off their findings to the next tier and return to their alert queue abyss. The in-depth learning and analysis will be done by someone with more experience, and the new analyst's understanding of the attack remains unchanged. This problem is further exacerbated as the team scales. A growing SOC adds more tiers to handle more alerts and the bureaucracy thickens, with the lowest level analysts losing scope with every new cog added to the triage machine. Given the level of fatiguing and tedium that comes with pure alert triage, can you blame that analyst for leaving after a year to pursue a development role somewhere else instead?

If this issue sounds familiar, consider that this scenario only highlights the plight of a new analyst. In the case of a more experienced analyst, add to the deluge of alerts each additional step for which he or she is responsible, including the actual investigations and remediation. With thousands of alerts being generated daily, it should be concerning yet unsurprising to hear that nearly one-third of organizations claim they ignore at least 50% of all security alerts because they simply cannot keep up with the volume. What ensues is a frantic game of catch-up that only increases the probability of human error over time.

37%

OF ORGANIZATIONS CITE KEEPING UP WITH THE **VOLUME OF ALERTS** AS ONE OF THE **BIGGEST** INCIDENT RESPONSE **CHALLENGES**

Achieving Speed

As an industry leader in the endpoint detection and response (EDR) space, Carbon Black has spent years redefining the very economics of security operations. When people and processes fall victim to today's tumultuous cyber landscape, Cb Response continues to reduce the cost, complexity, and time of traditional security operations and incident response.

Working with some of the most experienced and highly-efficient SOCs internationally, Carbon Black has purpose-built Cb Response for SOC and IR professionals to enable them to proactively hunt for threats in real-time. Over the years, Cb Response has consistently empowered SOCs to make the most of the people and resources they have by leveraging automation and orchestration for rapid security decision-making.

A high-speed SOC must excel in many different areas of security operations to ensure that valuable time is not handed over to the adversary. It is crucial for security professionals to understand that the ability to operate an agile, intelligence-driven SOC is dependent on your organization's answer to the following five questions.

1. WHAT ARE THE BASICS WE NEED TO MASTER FIRST?

Speed is only built on a strong security foundation. A process is only able to be automated once it has been perfected by your team. Automating a process that your team does not fully understand will create blind spots and likely decrease your visibility as you attempt to scale. Before tasking machines with processes that are key to your security, make sure you understand all the weaknesses of your current posture.

- Have you minimized your attack surface?
- Have you inventoried every asset?
- Are your systems being properly patched?
- How would you know if they were not?

> Nowadays, we are able to detect and respond even before the user contacts us. To date, we have reduced the IR time from days to hours."
>
> *- Ismael Briones-Vilar, Senior Security Analyst, Inmarsat*

These questions may have more in common with basic IT hygiene than security, but they are essential to the success of your SOC. Using Cb Response, our customers enjoy complete visibility across their environment to continuously monitor every detail of every event.

We asked Ismael, a senior security analyst at a firm operating a global network of telecommunication satellites, how he uses Cb Response to master the basics of security and achieve speed. "Carbon Black has decreased the time required to identify and respond to a security incident. Before Cb Response, we required hours or days before we could identify an endpoint compromised by a zero-day in Microsoft Word, for example, often because the affected user notified us about a suspicious document or PDF. Nowadays, we are able to detect and respond even before the user contacts us. To date, we have reduced the IR time from days to hours."

2. HOW CAN I EFFICIENTLY ORGANIZE AND LEAD THE PEOPLE ON MY TEAM?

Organizing your team to protect your environment with agility is a difficult task with all the varied skills and challenges related to traditional SOC structures. We asked our partners at Red Canary, who every day provide security solutions that harness the visibility of Carbon Black's products, to share how they keep up with the constantly evolving functions of today's intelligence-driven security teams.

"At Red Canary, efficiency starts with breaking down the structures seen in traditional SOCs. We have found the most success by moving beyond an operation that focuses solely on event analysis. To do this, we include our Intel team in engineering efforts, engineers in analysis efforts, and so on. Rather than assigning each team member a label to exclusively focus on, each person has a core 'practice.' They still develop and improve within their practice, but they are also challenged to engage with other functions in the SOC.

“This approach completely bucks traditional views of security operations, and has led to amazing innovation within our security team and around the investigation process. Our engineers are actively examining the analysis process, seeing the results, and continuously working to develop efficiencies for our analysis team. This approach has led to data analysis and automation efforts that have removed the need for in-depth investigation in nearly 10% of all threats. It has led to effective suppression that provides each individual analyst with the ability to ‘tune’ detection criteria during an investigation. That tuning is then used to automatically suppress potential threats in the future. Doing so has enabled our analysts to be **4-5X more efficient** over the last three years, and much of this can be attributed to how we evolved our security team by removing more traditional, time-intensive job functions.”

3. HOW CAN TECHNOLOGY HELP STREAMLINE OUR DETECTION AND RESPONSE PROCESSES?

Complete control starts with complete visibility over your endpoints. Being able to quickly detect an attack depends on how centralized all your data is. Cb Response works with your current SIEM and many other elements of your security stack to ensure that every system event is recorded continuously and readily available for you to visualize when an investigation is necessary. At a glance, analysts also have instant access to a readout of endpoint health and your SOC’s key performance indicators.

Proactively hunt threats across your enterprise. With Cb Response you can explore your environment, discover threats missed by outdated detection methods, and reduce attack dwell time. Security professionals use Cb Response to validate their hunting hypotheses and create automated watchlists to generate custom alerts for suspicious patterns they identify. We asked Dan, a cyber defense analyst at Motorola Solutions, how he uses Cb Response to rapidly uncover threats from a single console and enable his organization to continue providing mission-critical communication products and services all over the world. “The time saved is immense, because Cb Response makes it easy to determine if a hit is a false positive or not. Usually, just looking at the command line, parent/child processes, and netconns will let you make an assessment.”

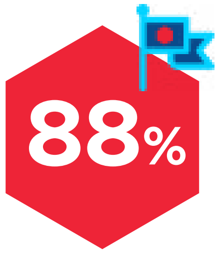
> “The time saved is immense because Cb Response makes it easy to determine if a hit is a false positive or not.”
>
> *- Dan Banker, Cyber Defense Analyst, Motorola Solutions*

Rapidly drill down to root cause. In the case of malicious attacks, it can take over 9 months on average to properly identify the root cause of an incident and contain it. Cb Response allows analysts to visualize the complete attack kill chain and then respond and remediate the attack within minutes, without having to manually aggregate and sift through relevant raw data post-incident. Cb Response allows you to safely isolate an infected host and then obtain secure direct access to that endpoint to continue your investigation. Our Live Response functionality enables IR professionals to pull or push files, run commands, and perform memory dumps, all from within a single console.

4. HOW CAN MY ENTIRE SOC EVOLVE WITH EVERY NEW ATTACK?

In a Verizon report, 88% of breaches fell into one of nine patterns that had existed three years prior. Attackers know that legacy antivirus products can be easily bypassed by making slight changes to avoid being identified as “known bad.” However, utilizing patterns of attack to connect the dots between IOCs and all other system events, SOC analysts and incident responders can gain complete understanding of the precise sequence of events as a cyber crime unfolds. There is clear cause-and-effect insight into where an attacker gained access, what he tried to accomplish, how he attempted exfiltration and, ultimately, what the exact root cause of the attack was. Without this contextual understanding of the attack, an incident responder would completely lack any additional insight into how the organization could be better protected in the future.

We asked Kevin, an IT director at an accounting firm using Cb Response, how he is able avoid addressing the same threats over and over.



OF BREACHES FELL INTO ONE OF NINE PATTERNS THAT HAD EXISTED THREE YEARS PRIOR.

Response provides a launch pad into researching where a threat exists, how it got there, and allows us to isolate it before it spreads."

- Kevin Kraft, IT Director, Bowman and Company, LLP

"Cb Response provides a launch pad into researching where a threat exists, how it got there, and allows us to isolate it before it spreads. We use Cb Response to greatly reduce the time spent investigating threats once they are detected and to provide us with a single interface to perform all investigative actions. Once a threat has been identified, we are able to construct a watchlist out of the events and processes associated with the threat. This allows us to have a 'fool me once, shame on you' posture to avoid being hit twice for the same or similar threat."

Continuous and centralized recording means Cb Response has every bit of data necessary to identify a pattern of attack and provide an intuitive visualization to identify root cause. Cb Response not only correlates indicators of compromise, it provides full context via a detailed attack chain with information about every process spawned and every endpoint affected. This detailed level of information is invaluable to closing the IR feedback loop, ensuring that everything you learn flows back into your SOC in the form of actionable intel that drives automation in the future. Cb Response helps you operationalize your new understanding of malicious techniques as automated watchlists enabling you to spend more time hunting new threats and less time constantly policing known areas of risk manually.

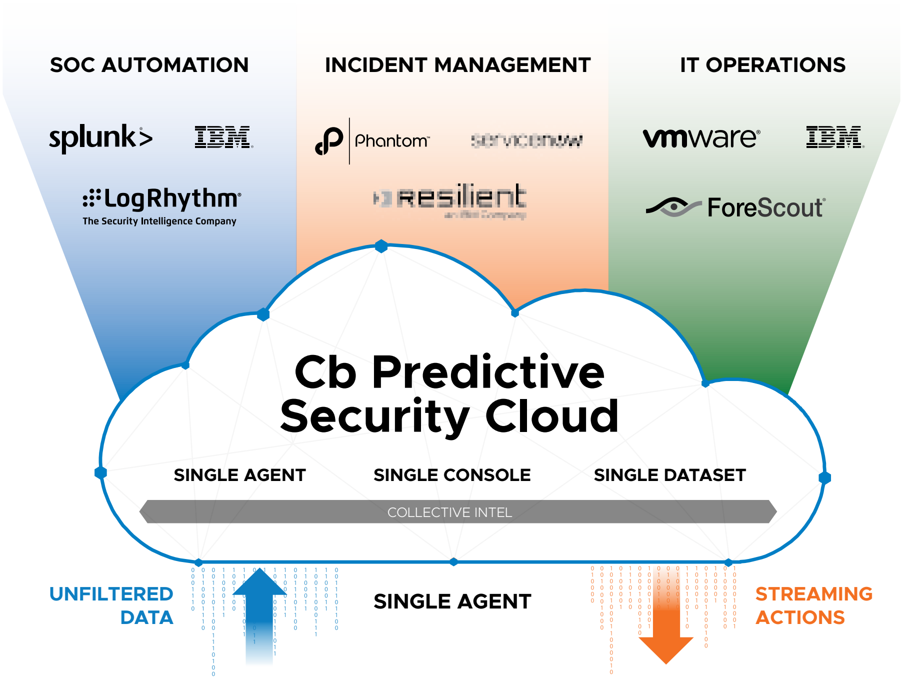
5. WHO CAN WE TURN TO FOR SUPPORT?

Corporate-minded cybercriminals collude every day to launch attacks on unsuspecting corporations. With more than 14 million endpoints now protected by Carbon Black globally, embracing collective defense is not only easy, but incredibly advantageous to your security posture.

Cb Response enables SOCs to collectively defend their organizations by streamlining the implementation of threat intelligence feeds through the Carbon Black Predictive Security Cloud. Cloud-based endpoint telemetry combines complete visibility with advanced intel and predictive analytics.

Big Data Meets an Open Platform

Both our on-premise and cloud offerings of Cb Response leverage the power of the Cb Predictive Security Cloud for rapid watchlist distribution and cloud detonation. Cb Response also leverages the Cb Predictive Security Cloud to enrich unfiltered endpoint data with the latest threat intelligence from Carbon Black or a custom third-party source. The result is the most robust cloud-powered intel available to help you stop the most attacks.



Join a Global Community of Experts

As the latest 2017 variant of the global Petya cyberattack made waves, hitting numerous organizations across the globe, Carbon Black's Threat Analysis Unit (TAU) worked through the night with over 100 Carbon Black customers, actively analyzing and sharing new insights and indicators of compromise. Hour by hour and hash by hash, over 4,000 security professionals absorbed all the latest intel available as seasoned experts weighed in for the benefit of the entire community.

> “The analysis & IOCs provided by security experts in Carbon Black's global community were most helpful… All IOCs were pre-banned across endpoints prior to infection.”
>
> *- Caleb Cromun, System Engineer, Samaritan Ministries*

Conclusion

Speed is the difference between a compromise and a breach. Reactively collecting data using antiquated forensic tools and outdated antivirus products delivers very little visibility into the complete context of an incident and often results in extra labor. It is impossible to know what exactly you will need to investigate an incident before it happens, but it is possible to minimize your detection and response times by arming your team with complete visibility.

Striking the balance of people, process, and technology to produce an agile, intelligence-driven SOC is no easy task, but with Cb Response you can rapidly evolve and harden your defenses with every new attack. Once you can streamline and automate that learning process, your people and your tools can proactively hunt for new threats faster than ever.

“

It is not strength that protects you, it's **agility.**
It is not compliance that assures, it is **discipline.**
It is not what you know, it's what you **do not know**
It is not skill that makes somebody qualified, it is **behavior.**

Future SOC is not technology, per se; it is people, intelligence, and automation for a rapid response to a threat."

Andrew Plato, CEO, Anitian
Discovered SQL Injection in 1995

Carbon Black.

Carbon Black is a leading provider of next-generation endpoint security. Carbon Black serves more than 3,700 customers globally, including 30 of the Fortune 100. As a cybersecurity innovator, Carbon Black has pioneered multiple endpoint security categories, including application control, endpoint detection and response (EDR), and next-generation antivirus (NGAV). Leveraging its newly introduced big data and analytics cloud platform – the Cb Predictive Security Cloud – Carbon Black solutions enable customers to defend against the most advanced cyber threats, including malware, ransomware, and non-malware attacks. Deployed via the cloud, on premise, or as a managed service, customers use Carbon Black solutions to lock down critical systems, hunt threats, and replace legacy antivirus. For more information, please visit www.carbonblack.com or follow us on Twitter at @ CarbonBlack_Inc.

1100 Winter Street, Waltham, MA 02451 USA
P 617.393.7400 F 617.393.7499
www.carbonblack.com