Carbon Black's experienced security experts add tremendous value to your organization by furthering your SOC's capability to rapidly and effectively detect and respond to security incidents. Our expert approach leverages your current Cb Response implementation and our best practice methodology to enable advanced methods of hunting, identification, triage and response to those events most impactful to your organization.

This offering enhances your security posture through several key activities:

- Optimizing your existing Cb Response capabilities to improve SOC operations to scope and gain visibility into the most impactful events to your organization and provide rapid response techniques to contain and minimize attack damage.
- Creating accurate, in-depth detection and monitoring of the kill chain to defend your organization against the many vectors an actor can leverage when attempting to compromise an environment.
- Improving analysis and response times through the correlation of threat intelligence and the data collected by the Cb Response sensor ecosystem.

Our approach is to bring our expertise to you, and sit onsite with your staff working shoulder to shoulder behind the keyboard to efficiently transfer our knowledge and best practices. The agenda for this offering is:

**GET PREPARED**
A remote session to review the Cb Response Advanced Consulting package and plan onsite logistics.

**GET SECURE**
2-day onsite workshop to:
- Review & tune existing Watchlists
- Implement kill chain detection capabilities
- Setup monitoring of high value assets
- Review alerts and Watchlist hits
- Demonstrate advanced “How To Hunt” techniques
- Leverage rapid response and triage methodology
- Cb Live Response functionality.

**STAY SECURE**
Post-onsite virtual touchpoints to maintain continuity and provide continued knowledge transfer:
- Up to four 1-hour virtual sessions that provide:
  - Ongoing coaching to review alerts and create additional Watchlists
  - Q&A based on topics originating from onsite workshop
  - Guidance using Cb Response to perform analysis on security events.

---

**Cb Response Advanced Consulting Package**

Customized tuning of your Cb Response detection platform delivered as 2 days of onsite, hands-on mentoring from industry-recognized experts.

---

**At a Glance**
- Two days of onsite, hands-on best practice mentorship. No “Death by PowerPoint!”
- Expert evaluation of current Cb Response detection & monitoring controls
- Customized kill chain detection workshop
- In depth “How to Hunt” methodology
- Incident Triage and Live Response working sessions
- Delivered by industry-recognized security SMEs
Participation Requirements

Given that this package is delivered as an intensive 2-day, hands-on workshop, we have several requirements for our customers before the onsite session:

**COMPETE & RETURN THE CB RESPONSE ADVANCED CONSULTING ENVIRONMENTAL CHECKLIST**
(along with specified environmental data provided during the initial planning call)
- Upload Cb Response logs to the Carbon Black Alliance Server
- Upload Cb Response Watchlists to the Carbon Black Alliance Server

**A MATURE, STABLE ENVIRONMENT**
- Minimum 60 days after initial professional services project is closed
- Any high-severity cases (P0 & P1) must be resolved

**ALL PREREQUISITE TRAINING COMPLETED**
- Responder Administration Training
- Response Advanced Analyst Skills Training

**EXPERIENCED CB RESPONSE AND SECURITY STAFF**
- Staff must spend a minimum of 4 hours/week using the Cb Response console
- Staff must be familiar with environment architecture, tools, and associated security and operational processes

**ADDITIONAL LOGISTICS**
- Minimum 3 weeks' notice to schedule onsite workshop
- The full schedule will be determined during the initial planning call, including the dates for the onsite workshops

Carbon Black is the leading provider of next-gen endpoint security. Carbon Black's Next-Gen Antivirus (NGAV) solution, Cb Defense, leverages breakthrough prevention technology, “Streaming Prevention,” to instantly see and stop cyberattacks before they execute. Cb Defense uniquely combines breakthrough prevention with market-leading detection and response into a single, lightweight agent delivered through the cloud. With more than 7 million endpoints under management, Carbon Black has more than 2,500 customers, including 30 of the Fortune 100. These customers use Carbon Black to replace legacy antivirus, lock down critical systems, hunt threats, and protect their endpoints from the most advanced cyberattacks, including non-malware attacks.