CB Response
Advanced Consulting Package

Hands-on mentorship and tuning for your CB Response environment delivered remotely or as a 2-day onsite from industry-recognized experts.

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 remotely (or onsite) with your staff to work shoulder to shoulder behind the keyboard to efficiently transfer our knowledge and best practices. The three phased agenda for this offering is:

Get Prepared
A remote session to review the CB Response Advanced Consulting package and plan delivery logistics.

Get Secure
Mentor Workshop Delivery (remote or 2-day onsite):

• Review & tune existing Watchlists
• Setup monitoring of high value assets
• Triage alerts and Watchlist hits
• Demonstrate advanced “How To Hunt” techniques
• Leverage rapid response and triage methodology
  – CB Live Response functionality.

Stay Secure
Post-workshop 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 workshop
  – Guidance using CB Response to perform analysis on security events.

VALUE AT A GLANCE

• Delivered remotely or via two days onsite, for 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 a concentrated, hands-on workshop by industry-recognized experts, we have several requirements for our customers before the working sessions component of this package can be delivered:

Complete and 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

• A minimum 60 days after initial professional services project is closed
• Any high-severity cases (P0 & P1) must be resolved

All Prerequisite Training Complete

• Responder Administration Training
• Response Advanced Analyst Skills Training

Experienced CB Response and Security Staff

• Staff must spend minimum 4 hours per week using the CB Response console
• Staff must be familiar with the 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 (if applicable)

About Carbon Black

Carbon Black (NASDAQ: CBLK) is a leading provider of next-generation endpoint security delivered via the cloud. Leveraging its big data and analytics cloud platform – the CB Predictive Security Cloud – Carbon Black consolidates prevention, detection, response, threat hunting and managed services into a single platform with a single agent and single console, making it easier for organizations to consolidate security stacks and achieve better protection. 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) enabling customers to defend against the most advanced threats. More than 4,300 global customers, including 35 of the Fortune 100, trust Carbon Black to keep their organizations safe.

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