Carbon Black.

Cb ThreatSight on the PSC

Managed Threat Hunting Service for Cb Defense

As enterprises face a shortage of skilled security professionals, security teams often spend too much time monitoring and validating alerts, which limits their ability to address other security needs. Moreover, when prevalent outbreaks occur, security team investigations are limited by the resources and data available in their own environment, making it difficult to craft an effective remediation plan until the full scope and root cause of an event is determined.

Cb ThreatSight helps solve these problems by providing an industry-leading, subscription-based monitoring service for Cb Defense. Built directly on the Cb Predictive Security Cloud™ (PSC) platform which applies big data analytics across unfiltered data from millions of endpoints, Cb ThreatSight is staffed by a world-class team of security experts who are constantly studying and analyzing the data in the PSC using advanced machine learning and algorithmic toolsets.

Offered as a managed service directly from Carbon Black, threat hunters on the Cb ThreatSight team work side by side with you to validate and prioritize alerts, uncover new threats, and accelerate investigations with capabilities such as predictive root cause reporting.

"Another kudo for Carbon Black. I follow Cb ThreatSight's recommendations immediately and it is already working. [They are] a superior team."

– CHUCK BALDWIN, IT ADMINISTRATOR, INTEGRA TECHNOLOGIES
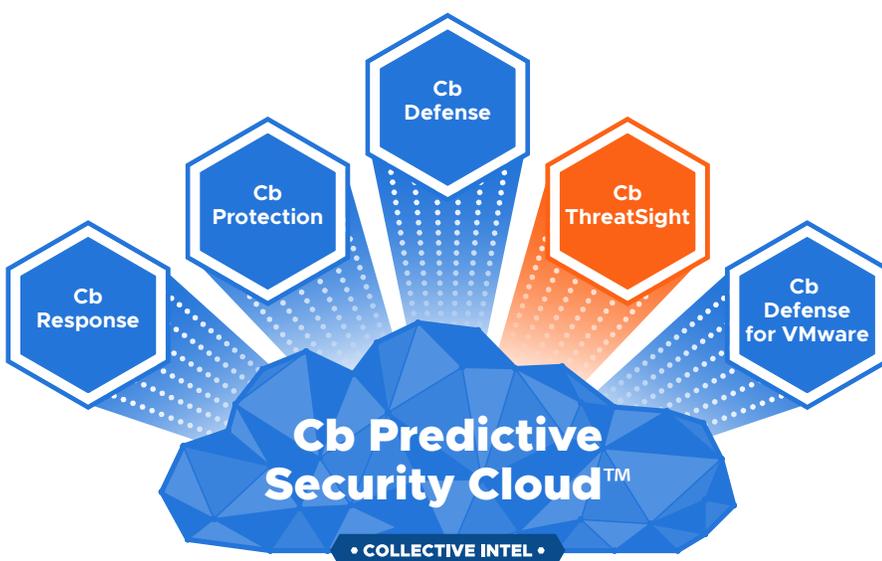
Use Cases

- Support for handling security alerts

- Extra set of eyes on your environment

- Security experts supplementing your team

Benefits

- More efficient and proactive security operations

- More actionable alerts, reducing alert fatigue

- Better alignment with executives through clear reports

- Reduced time spent investigating root cause

- Alleviation of staffing pressures with 24x7 support

- Clearer view of security trends to help guide policy

Cb ThreatSight and the PSC

- Human analysts use the PSC's unfiltered data to hunt evasive threats

- Global threat intel allows us to see attack trends before they hit you

- Monthly reports provide additional insights about your environment

Cb Defense · Cb Protection · Cb ThreatSight · Cb Response · Cb Defense for VMware

Cb Predictive Security Cloud™

• COLLECTIVE INTEL •

Key Capabilities

Threat Validation and Insight

With round-the-clock eyes on glass, your team can have true peace of mind knowing that an additional layer of experts are helping to ensure threats don't get missed. Carbon Black's security experts work side by side with your own team to validate alerts and provide additional human insight to speed up remediation for improved stability and resource utilization.

Monthly Reporting

Our Cb ThreatSight experts provide monthly reports that summarize monthly activity across your environment, including the most common suspicious events and most targeted machines. These reports serve as a starting point for refining policies, help your team see big picture trends and make executive reporting effortless.

Outbreak Advisories

Carbon Black's Threat Analysis Unit constantly monitors threat trends across the globe. When widespread and newsworthy outbreaks occur our ThreatSight team sends out advisories that include indicators of compromise, giving your team a jump-start on assessing risk and closing gaps.

Features

- Threat validation
- Email alerting
- Root cause analysis
- Threat advisories
- Monthly reporting

Platforms

Cb ThreatSight is an add-on to Cb Defense, which supports

- Windows: Windows 7/8/10
- Mac OS X: 10.6.8+
- Server: Windows 2008
  Windows 2012
  Windows 2016

When the Cb Threatsight team validates a true threat, they immediately notify your administrators and provide additional context to help streamline investigations and resolve issues faster.
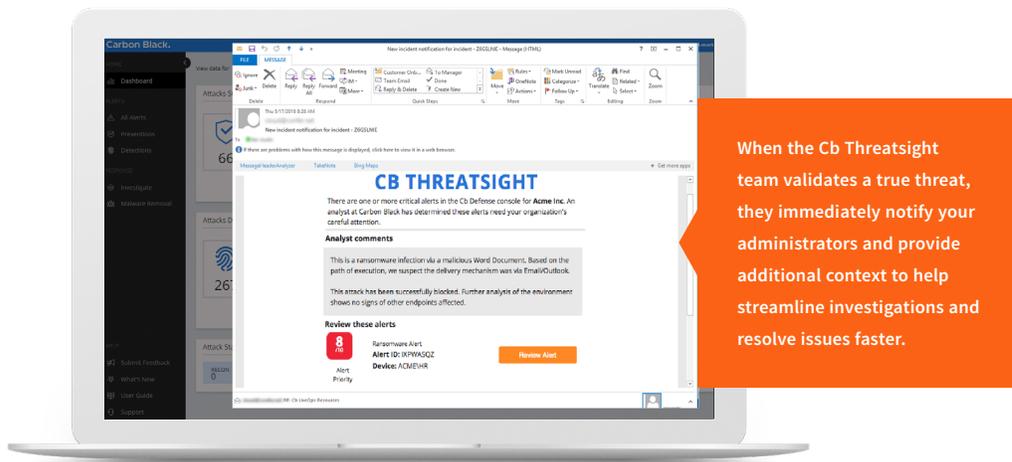
About Carbon Black

Carbon Black is a leading provider of next-generation endpoint security. Carbon Black serves more than 3,700 customers globally, including 33 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.

Carbon Black.