Carbon Black Introduces Cb LiveOps for Real-Time Query and Response, Surpassing Tanium and CrowdStrike With Its Complete, Cloud-Delivered Security Platform

Submitted by: C8 Consulting
Thursday, 2 August 2018

Cb LiveOps is built on an industry-leading security platform that combines real-time query and response, next-generation antivirus, endpoint detection and response, and managed threat hunting services within a single console and from a single agent

Reading, UK — 2nd August, 2018 — Carbon Black (https://www.carbonblack.com/) (NASDAQ: CBLK), a leader in next-generation endpoint security, today announced the release of Cb LiveOps™ (https://www.carbonblack.com/products/cb-liveops/). Cb LiveOps extends core functionality of osquery (https://osquery.io/) to empower organisations to ask questions of all endpoints, take action to remediate identified issues in real time, and simplify operational reporting. It is the newest offering built on Carbon Black's groundbreaking Cb Predictive Security Cloud™ (PSC) (https://www.carbonblack.com/products/cb-predictive-security-cloud/), a platform that delivers complete endpoint prevention, detection, and response, all from a single agent.

Delivering Cb LiveOps on the PSC gives customers a consolidated and comprehensive, cloud-delivered security stack, one that bridges security and IT operations. As a result, organisations can move away from existing offerings in the market, such as those offered by Tanium and CrowdStrike, to a solution that delivers a full suite of functionality serving both security and IT teams. With Cb LiveOps, security teams can perform in-depth investigations, conduct remote remediation from the cloud, and perform on-demand vulnerability assessments, all within a single solution.

"We are excited to see Cb LiveOps change the game for security operations," said Ryan Polk, Carbon Black's Chief Product Officer. "To date, there has been a gap in security platforms, which lack the ability to make real-time inquiries across the entire endpoint fleet. By leveraging and extending osquery, the open-source tool used by hundreds of the world's largest enterprises, we are filling this gap, delivering what we believe is the most complete security platform, which combines advanced prevention, detection, response, and IT operations delivered from the same agent, same login screen, and same UI as all other Carbon Black offerings on the PSC."

_____

Tweet this: Real-time query + response, NGAV, EDR, and managed threat hunting from a single platform, with a single agent and single console? You asked, we delivered! @CarbonBlack_Inc's Cb LiveOps leverages #osquery to give #secops a complete cloud security platform http://ow.ly/GAyO30ldJJg

_____

"Cb LiveOps enables our incident response (IR) team to acquire key forensic artifacts that normally would require additional collection and offline parsing," said Tim Stiller, Senior Incident Response Consultant at Rapid7. "It allows our teams to scale out our response from one to hundreds of systems. This allows us to quickly scope out an engagement to determine root cause."

Cb LiveOps provides additional value in bridging the gap between security and operations and empowers IT

administrators to provide ROI well beyond the typical security use cases including: immediate IT hygiene analysis, on-demand compliance audits, and seamless asset management.

New Use Cases Enabled by Cb LiveOps

• Inspect Endpoints in Real Time: Security analysts need immediate answers to critical questions across their entire fleet of endpoints during attacks. Cb LiveOps provides access to more than 1,500 unique endpoint artifacts to help analysts discover and analyze attacks to respond to incidents at a whole new level. For example, if during an investigation the security team determines that credentials have been stolen, Cb LiveOps can query all endpoints to see if, and where, the credentials have been used for attempted logins, and if, and where, these credentials are currently in use.

• Verify Patch-Level Compliance: Security and IT teams can use Cb LiveOps to automate queries of all endpoints and determine if all machines are at the right level of compliance. Additionally, to meet real-time or ongoing reporting needs, teams can use Cb LiveOps to automate operational reporting on patch levels, user privileges, disk-encryption status, and more.

• Remediate Attacks in Real Time: Once an attack is identified, Cb LiveOps allows administrators to open a session within seconds to terminate processes, delete files, or execute a background process to remediate the threat in real time – no matter where the compromised endpoints are located, eliminating uncertainty and greatly reducing any downtime that results from an attack.

“There is a need for a combined strategy between IT and security,” said Carl Erickson, Head of Information Security at Signify (previously Philips Lighting). “Cb LiveOps is directly in line with what is required from SOC analysts. The ability to actually do live queries rather than rely on teams to use existing data is a big step forward.”

Resources

Cb LiveOps Blog
(https://www.carbonblack.com/2018/08/02/carbon-black-announces-cb-liveops-a-new-offering-on-the-cb-predictive-security-cl
Webinar: How to Bridge the Security and Operations Gap
(https://www.carbonblack.com/resource/operationalizing-threat-hunt/)
Learn More About the Cb Predictive Security Cloud (PSC)
(https://www.carbonblack.com/products/cb-predictive-security-cloud/)
Follow @CarbonBlack_Inc on Twitter (https://twitter.com/CarbonBlack_Inc)
Report: China, Russia & North Korea Launching Sophisticated, Espionage-Focused Cyberattacks
(https://www.carbonblack.com/2018/07/19/carbon-black-report-china-russia-north-korea-launching-sophisticated-espionage-fo
Stay up to date on the Carbon Black Blog (http://carbonblack.com/blog)

About Carbon Black

Carbon Black (NASDAQ: CBLK) is a leading provider of next-generation endpoint security. Carbon Black serves more than 4,000 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 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.

Contact

Paula Elliott
C8 Consulting
paula@c8consulting.co.uk
0118 949 7736

Michael Bartley
C8 Consulting
michael@c8consulting.co.uk
0118 949 7750