

Carbon Black and IBM Security Deliver Increased Visibility for SOCs to Accelerate Incident Response

Submitted by: C8 Consulting

Tuesday, 10 October 2017

IBM Resilient and Cb Response jointly integrate to strengthen enterprise continuity during cyberattacks

CB CONNECT CONFERENCE – Reading, UK - 11th October 2017 – Carbon Black, the leader in next-generation endpoint security, today announced an expansion of its collaboration with IBM Security [NYSE: IBM] via further integrations between their respective portfolios of cybersecurity tools. The new integration will connect customers that leverage both Carbon Black's market-leading endpoint detection and response (EDR) solution, Cb Response, with IBM Resilient's advanced Response Orchestration Platform, empowering security teams to respond faster and more comprehensively to modern cyberattacks.

With this announcement, joint customers of Carbon Black and IBM Resilient can use the products in a tightly integrated way. Security Operation Centers (SOCs) can automate remediation tasks and orchestrate critical incident response activities, creating a streamlined, agile response function. The power of the combined technologies ensures security teams can keep up with the evolving nature of cyberattacks and efficiently respond to incidents.

Today's businesses often depend on many different security solutions to protect their environments. Additionally, various departments (SOCs, IT, operations, HR) must work collaboratively to keep up with the speed of business.

The native integration enables users of both IBM Security and Carbon Black to automatically enrich new security incidents with deep endpoint data from Cb Response into the Resilient platform. Users can also leverage industry-leading threat intelligence, and remediate issues by banning malicious files.

This latest integration between Carbon Black and IBM Resilient benefits SOCs by allowing them to:

- Respond faster and more efficiently to incidents
- Gain enterprise-wide visibility via a hub for all incident response
- Free-up critical analyst time from mundane tasks to enable them to focus on the response
- Automatically collect and integrate endpoint data
- Enable high-speed SOC orchestration of endpoint remediation actions

"We are excited that IBM Security has expanded its partnership with Carbon Black," said Tom Barsi, senior vice president of business and corporate development for Carbon Black. "The combination of Cb Response and Resilient's leading orchestration response platform brings additional strength to SOCs and empowers security teams around the globe to automate remediation of advanced threats instantly."

"Carbon Black and Resilient together are providing a powerful way for organisations to fight against end point attacks that continue to plague organisations," said Ted Julian, VP of product management for IBM Security. "Carbon Black's Cb Response provides a complete view of what's happening across the enterprise. With the integration into Resilient, security teams can take action on that insight by orchestrating their response to any incident affecting the endpoint directly from the platform."

The option to integrate between Cb Response and IBM Resilient is the latest combined offering from Carbon Black and IBM Security. Among the additional elements of the partnership are:

IBM Services

Continuous Monitoring and Threat Response— IBM Security utilises Cb Response and Cb Defense to deliver a number of managed and consulting services to organisations worldwide. The managed detection & response service from IBM is a fully managed service that leverages Cb Response and intelligence from IBM X-Force research and experienced threat hunting teams to achieve continuous, real-time monitoring of enterprise endpoints for signs of malicious activity. In addition, Endpoint Managed Security on Cloud from IBM utilises Cb Defense to deliver managed next-generation anti-virus services for organisations that need to replace their aging antivirus solutions to better protect their endpoints. IBM also offers consulting services and incident response services that leverage Cb Response and Cb Defense that can be tailored to an organisation's needs.

Technology Integrations

QRadar Integration—The Carbon Black App for IBM QRadar provides a turnkey solution for integrating Carbon Black's products with IBM Security intelligence technology to provide organisations with a single pane of glass to more quickly detect and respond to security alerts. QRadar dashboards specific to Carbon Black eliminate the need for analysts to swivel across systems as data flows in. This app is provided at no charge to Carbon Black and IBM customers.

BigFix Integration— Seamlessly integrates prioritised patching, compliance, operations, and EDR. Through this solution, analysts leverage BigFix and Carbon Black to disrupt attacker behaviour using a closed-loop endpoint security and management system to detect and respond to attacks in progress and then quickly close exploited vulnerabilities by applying targeted patches across all endpoints in minutes. To help security professionals streamline and prioritise which threats and compromised apps to remediate first, the solution enables prioritised patching and accelerating the remediation of vulnerable endpoints, and brings down the cost of security.

About IBM Resilient

IBM Resilient's mission is to help organisations thrive in the face of any cyberattack or business crisis. The industry's leading Incident Response Platform (IRP) empowers security teams to analyse, respond to, and mitigate incidents faster, more intelligently, and more efficiently. The Resilient IRP is the industry's only complete IR orchestration and automation platform, enabling teams to integrate and align people, processes, and technologies into a single incident response hub. With Resilient, security teams can have best-in-class response capabilities. IBM Resilient has more than 200 global customers, including 50 of the Fortune 500, and hundreds of partners globally. Learn more at www.resilientsystems.com.

About IBM Security

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research, enables organisations to effectively manage risk and defend against emerging threats. IBM operates one of the world's broadest security research, development and delivery organisations, monitors 15 billion security events per day in more than 130 countries, and holds more than 3,000 security patents. For more information, please visit www.ibm.com/security, follow @IBMSecurity on Twitter or visit the IBM Security Intelligence blog.

About Carbon Black

Carbon Black is the leading provider of next-generation endpoint security. With more than 9 million endpoints under management, Carbon Black has more than 3,000 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.

Contact

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

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