·III Recorded Future®



Recorded Future for VMWare Carbon Black Cloud

Detect and respond to threats faster with actionable context at your fingertips. Our integrations with VMWare Carbon Black Cloud allow security teams to access the real-time information they need to detect incidents earlier and prioritize their findings with confidence, whether in the Recorded Future platform or VMWare Carbon Black.

Real-Time Threat Detection

Contextualized intelligence is a crucial component of any truly proactive security strategy. Recorded Future empowers faster, more informed security decisions with relevant insights that are updated in real time and integrated with your existing infrastructure. Security intelligence from open, technical, and dark web sources help reduce security risk by automatically correlating against telemetry data within your Carbon Black Cloud environment for realtime detection of potential threats.

Use Cases

Threat Detection

The explosive growth of indicators makes finding the needle in the haystack extremely resource-intensive for already overwhelmed security teams. With Recorded Future intelligence, security teams using Carbon Black can easily detect emerging threats using Recorded Future's malicious indicators.

Vm Carbon E	Black	Cloud				Notification -	
C b-internal-alliance	WATCHUSTS Denot and request in parential threats with automatable watchings. Leave more						Add Watchileta
b Dastonard	Show hits over: 3 days			RecordedPutureRiskyIPs This is the head with all all the roley go fram Recorded Future			Take Action
	TYPE © NAME © HITS ♥ Corbox Back Alexitant D						
		Carbon Black Carly		(Nerts Of			
	14	Acress Indicatory		(Service) Alere Ut			
	1	Carbon Black Rhown IOCs		Potest			
Enforce -	1.0	Carbon Black SANS		6 Reports			
	10	Lattine Sandbox Detonations	3.82	Sounce	NAM		SEVERITY
	1.0	Proofpore Malcoux	1		19990		
Reputation Malarate Demonst	1	Atachments		hecordedfuture	Photong Heat		
Dout Analysis	1.	Recordeans					-
	1.1	Recordedfuturelliskylt ashes	1.14	Gal RecordedFulture	Recently Reported by Inside Group		
		RecordedFutureRoligi#		D Received dury	Durrent DMC Server		
	1.	SAPTEST		Accorded Salar	Recard Positive Maleure WerSet		
	1	Text Watchilet					(Read)
	1	Resultance - Carbon Black		Recented Facure	Actually Communicating CAC Server		
	×	US Cybertom Malware Alam	<	E Recerted Aver	Recent Ballinet, Nutlic		
	1.1	Wilkey Connector					
// Column	1	Wind		Shewing 1-6 of 8		tharms per page 50	Despirate and the second

MWare[®]

BENEFITS

- Detect previously unknown threats
- Respond to findings faster
- Maximize investments in Carbon Black
- Accelerate security operations workflows

KEY FEATURES

- Recorded Future's risk lists for IPs, hashes, domains, and URLs
- Out-of-the box correlation detections against the client's endpoint data in VMware Carbon Black Cloud
- Leverage your Carbon Black investment right in Recorded Future by querying your client logs to see if a particular IOC exists

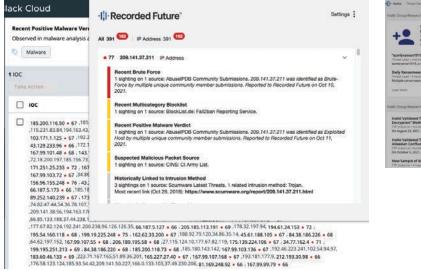


Enrichment

For even further context users can utilize Recorded Future's free browser extension with Carbon Black, allowing users to enrich findings with evidence-based, real-time risk scores and risk rules – all without having to leave Carbon Black. This empowers users to confidently prioritize, triage, and take action on the most important findings in their environment, simplify workflows, and maximize the ROI of existing cybersecurity solutions.



Joint clients also have the ability to leverage their VMware Carbon Black investment directly within Recorded Future with an Intelligence Card Extension. This extension combines external threat intelligence from Recorded Future with internal telemetry date for fast and informed decision making. By leveraging this extension clients can automatically check to see if an IOC exists in their log history, from within Recorded Future.



At Group Research Launa	· Carbon Black.	nurly Aerts
Top Story: RedLine Steals for Criminal Shops Voltage Top Professional and	Table Develop 118 Search results perced: New 2021-10-01 2015/46 to 2021-10-08 2015/46	0
RedLine Stealer is an infustealer -	 West Becards in last 7 days (Van of 30 choset) 	64.
coveral forums by the Russien-up	 Record Investiging: 2021-10-20120-20-46.3852, Device: chemitargel 1 	(04)
tombraman1919" Selling Mexican Airlines D. Troat Lout: - she hour ago contraman1519, a member of the mid-ter Raid Foxu	Proven Unichen Inputienten (MARTID_2000TL_ANF ingenen Texes 30211-66-00123-09.34 Envitted Event Type: Metamen	All unreads of \$1 priority areas. In the last 7 sizes.
ally Ransommare Roundup: 23 New Victims meat Date 4 Nouro ago hatiple ransommare threat actor groups published in	Evented from type: NETWORK Such 10/D: 2005/00/00/00/00/00/00/00/00/00/00/00/00/	avers. Assumed to Me
aat Silore	Francis and the CWIndowingstendZinchostane Anetosis	
	Process Name chaindows/aysterk32/sachotLave Roskend Tenestang: 2021.06-36123 Wells UM2	
t Group Research Tools and TTPs	Process Guil: 7053964-0035191 00000448-0000000-147804498484848	0
sikt Validated TTP: LockFile Ransomware Er		U
ncryption" Method, Variant Emerges 17 Instance - Insuring Package - Mills Acte - 3 Insurs 9 August 23, 2021, Insilet Group reported (see Valida	+ Record Simestamp: 2021-16-08720-20146-5852, Device: kogmoststeen-2	Rearrant of Responding on Print Party
nikt Validated TTP: PoC Exploit for CVE-2021 flassian Confluence shared on ExploitDB	Record torestamp: 3021-16-08720.38:35.8237, Device: ulTenhesi2	A reason in a subgradie of a line and control
F Instance - Hunting Package - SNORT Rule - 3 hour October 5, 2021, Mayara Deshmakh shared a pro	 Record towestamp: 2821:16-38722-38-76,8742; Device: mestading:tk2-wintfle 	nd Unanigned Alerts
w Sample of BigLock Ransomware Shared	 Record Immestamp: 2521-16-08720.3446.0152, Device: ctx310 	-

Results*

Resolve Security Threats 63% Faster

Relevant insights, updated in real time, and integrated with Carbon Black drive faster, more informed security decisions. Recorded Future eliminates laborious manual collection by providing contextual intelligence on internal telemetry data – empowering teams to quickly and confidently respond to incidents.

Identify 22% More Security Threats Before Impact

Using a sophisticated combination of patented machine and expert human analysis, Recorded Future fuses an unrivaled set of open source, dark web, technical sources, and original research to deliver relevant cyber threat insights in real time – empowering you to identify threats faster.

*Learn more about the business value Recorded Future brings to clients in our IDC Report

ABOUT RECORDED FUTURE

Recorded Future is the world's largest provider of intelligence for enterprise security. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future delivers intelligence that is timely, accurate, and actionable. In a world of ever-increasing chaos and uncertainty, Recorded Future empowers organizations with the visibility they need to identify and detect threats faster; take proactive action to disrupt adversaries; and protect their people, systems, and assets, so business can be conducted with confidence. Recorded Future is trusted by more than 1,000 businesses and government organizations around the world.

www.recordedfuture.com

