

Comodo and CybrHawk Announce Technology Partnership

COMODO

CybrHawk Integrates Comodo's OpenEDR Into XDR Solution Set

NEWS RELEASE BY COMODO

Clifton, NJ | December 15, 2020 10:03 AM Eastern Standard Time

Comodo, the world's leader of next-generation cybersecurity announced a technology partnership with CybrHawk, which operates the world's most advanced enterprise cybersecurity threat intelligence tools.

CybrHawk, a provider of XDR solution sets, recently integrated Comodo OpenEDR into its SIEM platform. "Comodo's OpenEDR is a 'gamechanger' for the Endpoint Detection and Response (EDR) market because it's just as capable as competing products like CrowdStrike's, but open source and free," said Jacob Thankachen, CEO & Co-founder at CybrHawk. He continued, "Plus, its modular approach gives customers the flexibility of replacing traditional antivirus for endpoints."

Comodo's **OpenEDR** is the world's most sophisticated and effective endpoint detection and response (EDR) available as open source. It allows you to analyze what's happening across your entire environment at the base-security-event level. OpenEDR has full-blown EDR capability and comes with seven days of log retention for free with the purchase of AEP.

Jacob continued, "Comodo's OpenEDR will be integrated with our 'pluggable' agent. The OpenEDR output will be shipped to CybrHawk XDR platform and will be used to monitor and alert on the activities. Based on the testing we've done, OpenEDR has accurate detection, with a low number of events, and is very lightweight. It has detected activities from the Atomic Red Team scripts and known viruses and the rate is 95%, same as CrowdStrike."

Comodo's EDR provides continuous real-time visibility of endpoints with detection and response. With the Open Source EDR product, an organization's IT team can identify attacks with the accurate root-cause analysis for effective remediation intelligence. It is a sophisticated endpoint agent that uses adaptive event modeling and allows logs to be sent to an elastic database and connect to systems like Kibana for visualization and reporting. In addition, a set of Indicators of compromise (IoCs) will be available and open for the community to create and deploy their own IoCs. An extensive rule engine will also be provided for collection of endpoint events, enrichment, and detection.

Alan Knepper, President and Chief Revenue Officer at Comodo commented, "We are offering our EDR as open source because we feel strongly that as cyber-threats increase, every company should have access to this capability regardless of budget or ability to purchase it." He continued, "We are putting an end to charging for multiple layers of security by open sourcing the world's most sophisticated EDR."

About Cybrhawk

CybrHawk is a leading provider of information-security-driven, risk intelligence solutions, focused solely on protecting clients from cyberattacks. We also pioneered an integrated approach that provides a wide range of cybersecurity solutions for organizations of varying size and complexity. Our solutions enable organizations to define their cyber defenses to prevent security breaches, detect real-time malicious activity, prioritize and respond quickly to security breaches, and predict emerging threats. For more information visit <https://cybrhawk.com/>



CybrHawk
Transforming Cybersecurity

About Comodo

Comodo is the world's leader of next-generation open source cybersecurity, with the industry's most disruptive innovations.

We help customers stop breaches with groundbreaking auto containment technology that neutralizes ransomware, malware and cyber-attacks. Our complete cloud-native framework delivers a zero-trust architecture with active breach protection for the most comprehensive defense against zero-day threats. Comodo's cybersecurity products maximize intelligent sharing between every component of the platform, therefore providing superior security. We are the only company that analyzes and gives a trusted

verdict for 100% of files on a network.

Comodo leverages innovation to celebrate and support the cybersecurity community by offering the very first open source endpoint detection and response (EDR). We believe that an open source model using community-powered collaboration will ensure that every organization has access to the industry's most sophisticated EDR.

Headquartered in Clifton NJ, Comodo's global development team and threat intelligence laboratories deliver innovative, category leading, security solutions for thousands of companies' endpoints, network boundaries, and internal networks. For more information visit <https://www.comodo.com/>

Contact Details

Carolyn Muzyka

+1 973-859-4000

carolyn.muzyka@comodo.com

Company Website

<http://www.comodo.com>

Tags

PARTNERS

PARTNERSHIP

ALLIANCE

RANSOMWARE

MALWARE

THREATINTEL

OPENEDR

EDR

ENDPOINTDETECTIONANDRESPONSE

- XDR
- CYBERSECURITY
- INFOSEC
- CYBERATTACKS
- CYBERPROTECTION