Technical Review

Comodo MDR: Security Operations Center-as-a-service

Date: November 2018 **Author:** Tony Palmer, Senior Validation Analyst; and Jack Poller, Senior Analyst

Abstract

This ESG Technical Review documents hands-on testing of the Comodo MDR security operations center (SOC)-as-a-service platform. We focus on how Comodo MDR provides defense-in-depth for organizations' network, endpoints, web, and cloud infrastructure as a bundled, cost-efficient service.

The Challenges

As ESG's annual IT spending intentions survey reveals, the global cybersecurity skills shortage continues unabated. In 2018, 51% of respondents state their organization has a problematic shortage (see Figure 1), up from 45% in 2017.[1] IT and security staff face an ever-growing amount of internally and externally generated data, hindering their ability to uncover and resolve threats quickly, and preventing them from keeping skills sets up to date. The skills gap threatens the ability of organizations to maintain effective security controls and minimize risk.

Figure 1. Top Ten Areas of IT Skills Shortage

Source: Enterprise Strategy Group

Organizations need effective cybersecurity management—aggregating data, prioritizing action, and distributing work—to handle the ever-increasing velocity and volume of cyber-attacks. Greater efficiency and automation can prevent organizations from being overwhelmed. Cybersecurity leaders who grasp the impact of the skills shortage should consider investing in developing skills and seeking products that improve operational efficiency. This may be why, according to ESG research, 36% of organizations stated that improving security and risk management was one of their top justifications for IT investments.

[1] Source: ESG Research Report, *2018 IT Spending Intentions Survey*, February 2018. All ESG research references and charts in this technical review have been taken from this research report.

The Solution: Comodo MDR

Comodo MDR is an integrated suite of managed detection and response technologies and services for advanced cybersecurity. The security operations center-as-a-service (SOCaaS) includes managed network (NDR), endpoint (EDR), web (WDR), and cloud (CDR) detection and response modules. Comodo MDR models operations on the NIST Cybersecurity Framework—standards, guidelines, and best practices to manage cybersecurity-related risk. NIST designed the framework to provide a prioritized, flexible, and cost-effective approach to promote the protection and resilience of IT infrastructure. This framework is organized around:

- **Identify**—Organizations can identify emerging threats using continuous log monitoring and behavioral anomaly detection integrated with external threat intelligence sources.
- **Protect**—Managed detection and response is layered on top of network, endpoint, cloud, and web detection and response and uses continuous monitoring as part of the defense-in-depth strategy to ensure perimeter, endpoint, back-end, and DMZ systems are free from compromise.
- **Detect**—Event correlations, behavioral analyses, real-time event processing, and correlation across all sensors enable detection of attacks.
- **Respond**—Preemptive containment technology, automation, and integration with various playbooks enable analysts to make the appropriate decisions, containing attacks and removing the possibility of attack propagation.
- **Recover**—Incident and case management services support enables onsite staff to manage the process of recovering from an attack.
- **Review**—Complete logging from event detection through response and recovery provide the mechanism for the cybersecurity team to review, adapt, and improve security and response for changes in adversary threats and techniques.

Why Comodo MDR?

ESG asked organizations what they felt were the three most important attributes of a cybersecurity platform.[2] Broad coverage across threat vectors like email and web (38%), central management across all products and services (33%), capabilities across prevention, detection, and response (31%), and coverage that spans endpoints, networks, servers, and cloud-based workloads (27%) were the top four responses. Cloud-based back-end services and tightly-coupled products and services—i.e., products and managed service options offering central command-and-control—were also cited.

ESG analyzed MDR offerings from five vendors including Comodo MDR to estimate the maturity level of the market versus Comodo's MDR offering. All vendors provided a few key features that can be defined as baseline MDR functionality. These features include managed network detection and response, integration with threat intelligence feeds, security monitoring, incident analysis, log data collection and correlation, and dedicated support staff. Comodo's global real-time support architecture includes 24x7 monitoring and detection at three unique global sites with five separate threat labs and is staffed by more than 150 cybersecurity experts.

Comodo has a more holistic view of what an MDR platform should be and has integrated all their technologies and products into the offering. There are numerous categories of functionality where Comodo MDR differentiates itself, detailed in Table 1.

[2] Source: ESG Master Survey Results, *Enterprise-class Cybersecurity Vendor Sentiment Survey*, October 2018

Table 1. Comodo MDR Service Analysis

Service	Other MDR Vendors	Comodo MDR
Managed endpoint detection and response	Other vendors we examined offer some level of managed endpoint detection and response.	• Base-event level environment analysis. • Granular root-cause analysis.
Managed application detection and response; Managed cloud detection and response	Most vendors we examined offer application and cloud detection and response.	• Monitors user access and security configuration changes. • Data loss prevention for cloud apps. • Threat and anomaly detection and remediation.
Managed web detection and response	No vendors we examined offer managed web detection and response.	• Web Application Firewall (WAF) provisioned over a Secure Content Delivery Network (CDN) • Staffed by certified security analysts in a 24x7x365 Cyber Security Operations Center (CSOC). • Powered by a SIEM that leverages data from over 85 million endpoints.
User and entity behavior analytics	Other vendors we examined offer some level of user and entity behavior analytics	• Profiling and alerting for anomalous behaviors and patterns on network, cloud, and endpoint assets.
Threat hunting	Other vendors we examined offer some level of a threat hunting service.	• Data visualization and analysis, statistical correlations, and data pivoting. • Base-event granularity to enable analysts to hunt for threats throughout the environment.
Incident response	Other vendors we examined offer some level of incident response.	• Multiple diverse techniques to disrupt and contain threats: APIs, watchlists, rules updates, isolation of processes or hosts from the network via endpoint agents, and/or locking and suspending user accounts.
Case management	Most vendors we examined offer some level of case management.	• Workflow integration tools prioritize alerts correctly to increase the speed and accuracy of remediation.
Pre-emptive containment	No vendors we examined offered pre-emptive containment.	• Comodo MDR offers a pre-emptive approach to containment, using the Valkyrie file verdict system to isolate unknown files on endpoints and return a fast decision.
Cloud-based SIEM	Some vendors we examined offer a cloud based SIEM, others rely on on-premises offerings.	• Event and forensic data across multiple network, endpoint, web, and cloud sensors are made available in a uniform log with a standardized visual interface. • Included in MDR with no licensing, infrastructure, or CapEx required.
AI support	Some vendors we examined leverage some level of AI and machine learning.	• Semi-supervised artificial intelligence engine. • Comodo's cybersecurity analyst decisions are fed into the AI intelligence engine to accelerate the detection and response to new threats.

Source: Enterprise Strategy Group

Comodo's goal is to redefine SOC operations, turning the current model on its head. Today, organizations employ numerous tier-1 cybersecurity analysts to monitor feeds and alerts from many independent tools from different vendors and sift through false positives, "screen watchers," if you will. Comodo MDR is designed to provide intelligent automation to enable

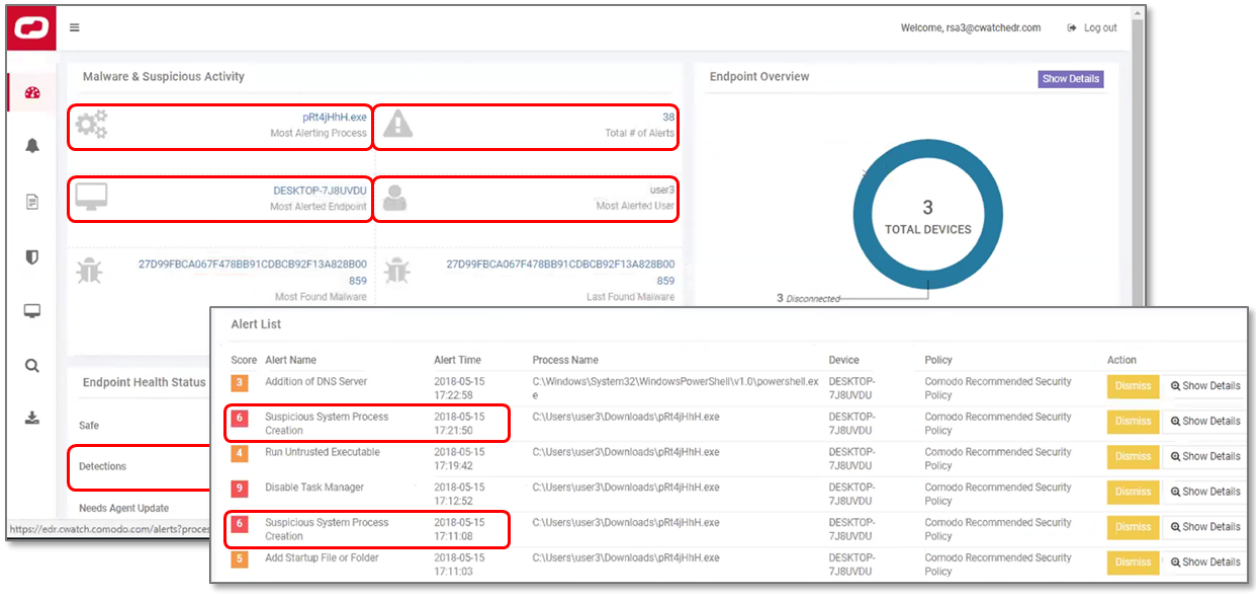
people to be deployed on more strategic and valuable tasks. Using Comodo MDR also enables organizations to extend their IT and security staff capabilities with Comodo's three-tiered analyst-supported SOC services.

Another important challenge for organizations is threats and attacks from outside their sphere of awareness. Organizations pay close attention to their own network and the devices and activity on it, but other attack spaces—the deep web and dark web, for example—might be completely invisible to them. Comodo MDR pulls data and intelligence from all areas into its platform to provide actionable intelligence to enable organizations to hunt for threats.

ESG Lab Tested

First, ESG looked at Comodo EDR with a goal of validating how it provides alerting for early warnings of known and unknown threats as well as detection of events and response. Comodo EDR requires a lightweight endpoint agent that consumes less than 1% CPU and 15-20MB RAM and can be deployed via group policy object (GPO) or by remote script execution on Comodo ONE, Comodo's remote monitoring and management platform. The EDR dashboard, seen in Figure 2, provides a summary view of malware and suspicious activity, including both early-warning alerts and detections of malware attacks. All are clickable links, enabling quick drill-down and investigation. In this case, we noted the most alerted endpoint, clicked on the total alerts link, and selected the endpoint to see the list of alerts associated with it.

Figure 2. The Comodo EDR Dashboard



Source: Enterprise Strategy Group

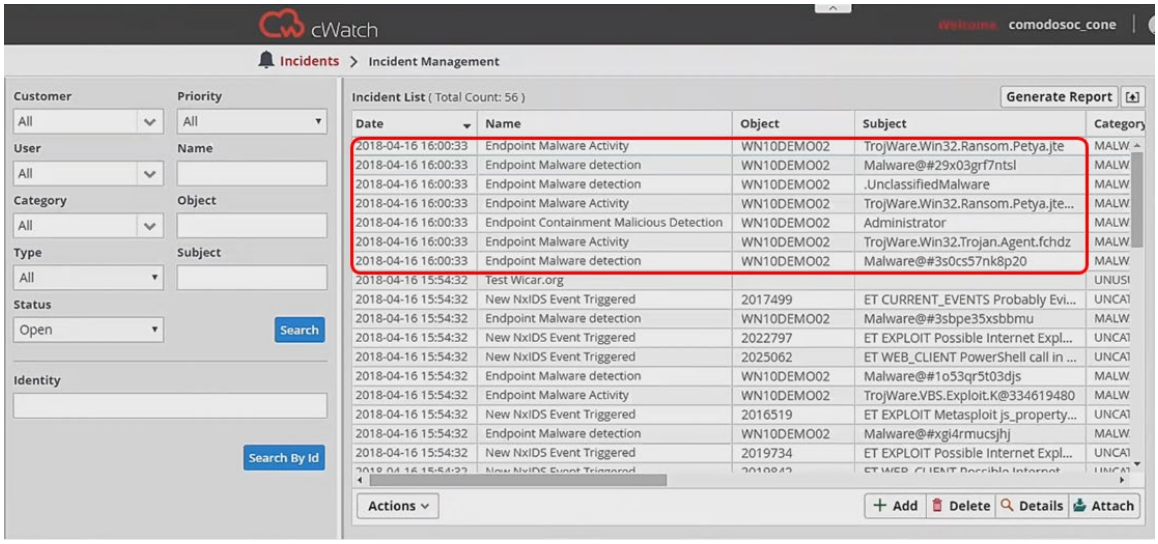
In the alerts, we selected the top suspicious system process creation alert and clicked ***details***. This showed us details on the file that created the suspicious process, including the file trajectory (i.e., movement of the file inside an organization), how the file operated (i.e., through PowerShell), and what specific commands were executed.

> EDR leverages Comodo's fully-customizable security policies. All license types come with Comodo's set of recommended security policies, but customers can customize security policies that alert on based on their business requirements.

There is a tremendous amount of additional detail and context provided by Comodo EDR that enables organizations to easily see which endpoints have executed this file and all the events the file has been involved in. This file was an unknown file when these alerts were generated, and EDR provided an early warning that enabled quick investigation and response. Next, we looked at how Comodo NDR works with on-premises sensors and other Comodo MDR components to collect and process logs and data from customer networks and automatically create incidents in the Comodo SOC. We

simulated multiple malware attacks on a test workstation running Windows 10 and the Comodo Internet Security client. We launched multiple malware attacks from the wicar.org website to observe how Comodo MDR integrates Comodo's suite of security offerings. Figure 3 shows the Comodo NDR dashboard after the malware payloads were detonated; incidents were generated automatically by the appropriate Comodo NDR component for detected malware, activities, behaviors, and intrusions.

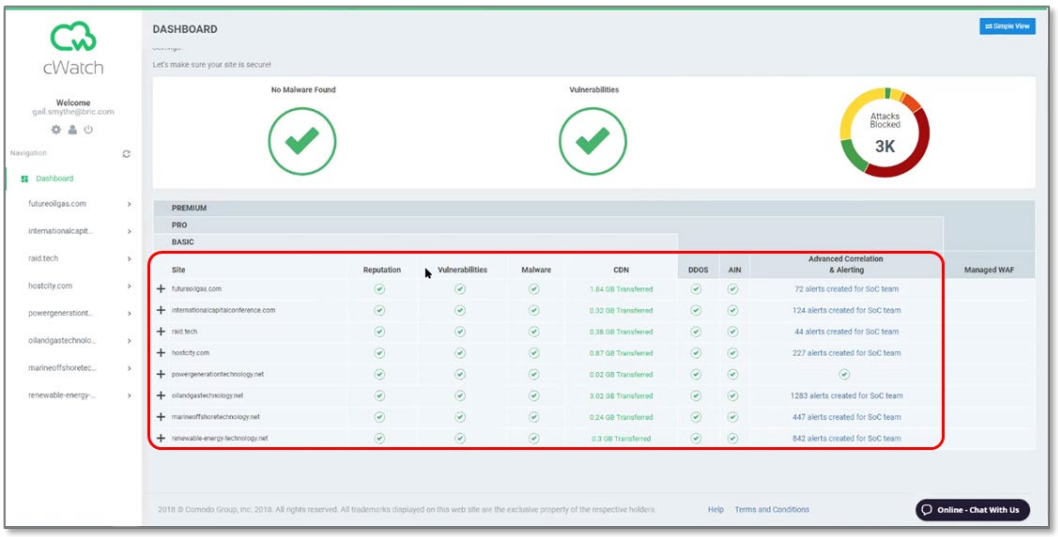
Figure 3. Automatically Generated Incidents in Comodo NDR



Source: Enterprise Strategy Group

Next, we looked at how cWatch Web enables organizations to protect their websites leveraging Comodo's cloud-based SOC. We logged in to the cWatch Web customer portal, seen in Figure 4.

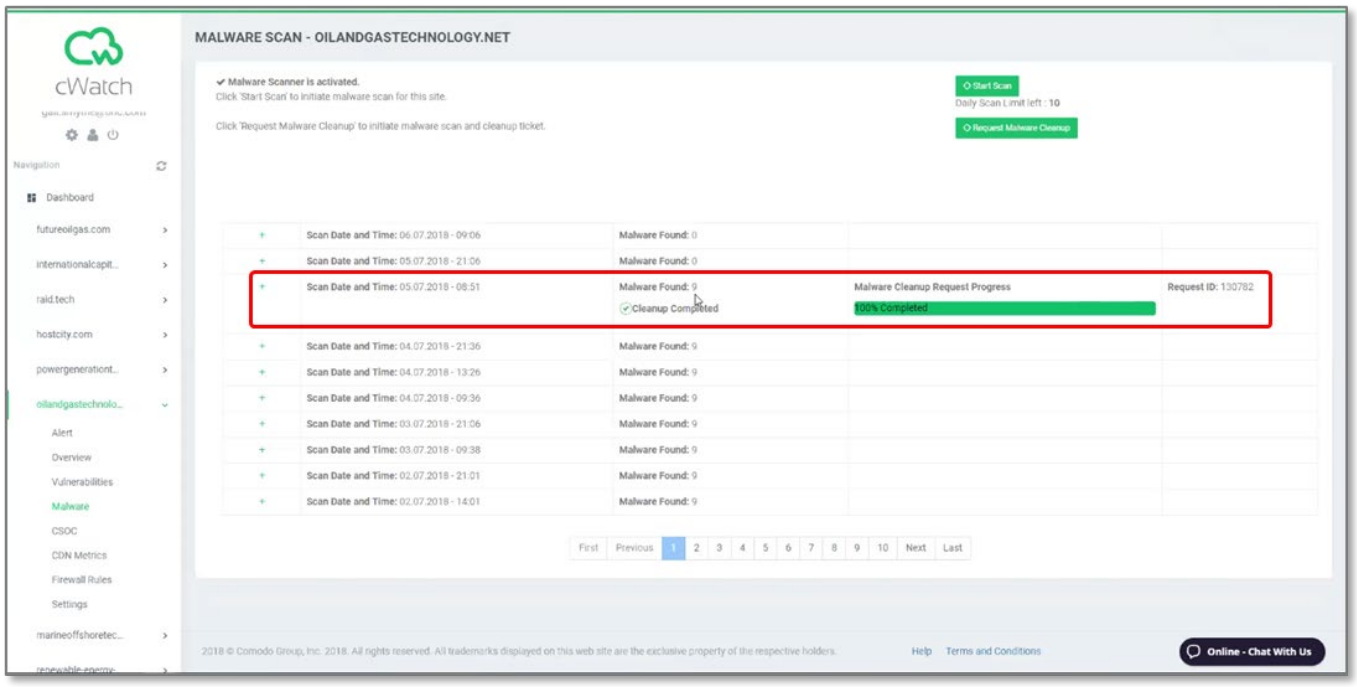
Figure 4. The cWatch Web Dashboard



Source: Enterprise Strategy Group

In the customer portal, organizations start with a summary view of their sites that are protected by cWatch Web. In addition to overviews of malware, vulnerabilities, and blocked attacks, an organization can easily drill down into any of its sites and learn more about any of the categories listed, such as reputation, malware, vulnerabilities, etc. We clicked on the site name *oilandgastechnoloy.net* and selected ***Malware.***

Figure 5. The cWatch Web Dashboard



Source: Enterprise Strategy Group

As Figure 5 shows, in a scheduled scan, nine instances of malware were found on this site. Behind the scenes, nine tickets requesting cleanup were automatically opened in the Comodo SOC, and all nine were automatically cleaned. cWatch Web also takes automated actions to address vulnerabilities in multiple categories and has the availability to virtually patch servers by creating targeted firewall rules to address open vulnerabilities until a patch becomes available.

ESG looked at multiple other components of the Comodo solution and how they integrated into the overall service. One example is Valkyrie, Comodo's cloud-based file analysis platform that provides static, dynamic, and human expert analysis for submitted known and unknown files. Valkyrie is the file analysis platform for all Comodo 360 network and endpoint solutions. Valkyrie's verdict-driven file analysis platform processes over 200 million unknown file submissions per day, uncovering more than 300 million unknown files every year leveraging integrated Comodo solutions, partners, and their active global community of threat researchers.

> Addressing malware on websites is very different from addressing malware on endpoints. Backdoors, code inserted into legitimate PHP scripts, and other non-executable components that are designed to deliver the payload would not be detected by traditional endpoint protection, which scans for executables and their behaviors.

Why This Matters

To address the cybersecurity skills gap, organizations need efficiency and automation for effective cybersecurity management if they hope to handle the ever-increasing velocity and volume of cyber-attacks without being overwhelmed. According to ESG research, 36% of organizations stated that improving security and risk management was one of their top justifications for IT investments.

Comodo has created an integrated, cloud-based SOCaaS offering that enables organizations to quickly and easily leverage the components they need—endpoint, network, web, cloud, or all four—along with Comodo's team of highly skilled security analysts to improve their security posture simply and cost-effectively.

The Bigger Truth

The ever-increasing volume and velocity of data, the shift to cloud architectures, digital transformation initiatives, and the growing sophistication of malicious actors are putting increasing demands on IT infrastructures, and high-performant cybersecurity solutions are often hampered by the increasing complexity of IT infrastructures. According to recent ESG research, more than two-thirds of surveyed organizations said that their IT environment has gotten more complex in the last two years. This complexity blurs the infrastructure perimeter, and makes it difficult to defend network, endpoint, cloud, and web workloads. Thus, it's no surprise that organizations are seeking to identify the best comprehensive security solution for their IT infrastructure.

When a security event hits, many organizations scramble for answers to questions such as:

- What happened?
- Who perpetrated it?
- Where did it occur?
- When did it begin?
- How did it happen?
- Why was it possible?
- And arguably the most important: What should we do now?

Effective incident response should handle all these questions quickly and effectively. ESG testing revealed that Comodo MDR enables organizations to quickly deploy and integrate a turnkey SOC for defense-in-depth protection of their critical assets (i.e., endpoints, networks, websites, and cloud resources), unifying all those different pieces under a common control framework and enabling organizations to not only be able to answer the questions listed above, but understand how to strengthen their security posture and prevent events in the future.

- NIST Cybersecurity Framework—Comodo MDR follows the well-known and well-regarded framework to identify, prevent, detect, respond to, and recover from threats and attacks.
- Improved economics—Comodo's SOCaaS delivers all features and functionality using an as-a-service model and reduces requirements for capital investments in cybersecurity IT infrastructure, software licenses, and the need for highly trained senior cybersecurity personnel.
- Global, real-time support— Comodo MDR uses a "follow-the-sun" model, with 24x7 monitoring and detection using three unique global sites, five separate threat labs, and more than 150 professionals and cybersecurity experts.
- Uniformity—Comodo MDR's security information and event manager (SIEM) makes all event and forensic data across multiple network, endpoint, web, and cloud sensors available in a uniform log with a standardized visual interface.
- Preemptive containment—Comodo patented technology preemptively contains and stops threats by denying malicious activity while allowing normal operations.
- Comprehensive coverage—Comodo MDR incorporates customer sensors for network, endpoint, web, and cloud workloads.
- Comprehensive threat hunting—Comodo provides a platform that delivers data visualization and analysis, statistical correlations, data pivoting, and other tools to enable security analysts to hunt for threats throughout the environment.
- AI guided MDR—Comodo's semi-supervised artificial intelligence engine learns from the activities and operations of Comodo's cybersecurity experts, accelerating the detection and response to new threats.

Organizations interested in automating the repetitive, tactical activities that consume their security teams today and move toward a proactive, intelligence-led model of prevention would be smart to explore how Comodo's MDR SOC-as-a-service can improve the operational efficiency of their cybersecurity teams, enabling them to rapidly and accurately answer those questions and improve their cybersecurity posture.