PERFORMANTA

Case study

Comprehensive 24x7 protection for a complex enterprise

International Healthcare Organisation

Endpoint Detection & Response (EDR)

Overview

- Recovering from several security incidents, an international healthcare organisation focused on improving its security estate.

- Performing gap analysis on the client's environment, Performanta uncovered several serious shortfalls, including no endpoint detection & response (EDR) services.

- To improve security coverage, we enrolled our client to Performanta's SIEM (Security Information and Event Management) platform. We also deployed our EDR solution, integrating it with our SOAR (Security Orchestration, Automation, and Response) service.

- Our healthcare customer now has 24-7 proactive and automated security coverage, and they saved 17 percent on their monitoring and response costs.

Executive Summary

Cybersecurity needs vary from organisation to organisation. But it's a rule of thumb that the larger an enterprise, the more complicated its digital systems. Criminals love complexity as it often leaves gaps to crawl through and lurk inside organisations. Such complexity can also undermine efforts to find the best security solutions.

Performanta's client, an international healthcare organisation, was very aware of these issues. It had suffered several security incidents and wanted to tighten its ship comprehensively. Yet even with this ambition, it failed to realise it had no endpoint detection & response (EDR) in place. Such an oversight is very common. Fortunately, gap analysis and security audits by Performanta uncovered such issues.

Once we understood our client's requirements, Performanta onboarded them to our SIEM (Security Information and Event Management) service. We also deployed an EDR solution and integrated it with our SOAR (Security Orchestration, Automation, and Response) service. To accelerate coverage, we added critical logs from the client, and to harden their posture, Performanta established Security Operations Centre and Incident Response processes and procedures.

Security solutions are readily available. But our healthcare customer required effective 24x7 threat detection and response capabilities that they could evolve and improve. Performanta helped them get there with our gap analysis, strategic engagements, and expertise in deploying and configuring different security services. Additionally, they saved 17 percent on their monitoring and response costs. Our client knew the stakes thanks to previous incidents; our solutions reinvigorated the confidence that they are in control and can spot and stop breach attempts.

The Challenge

This healthcare organisation had previously encountered breach incidents and wanted to improve their security posture. Their plans included adopting better detection and response capabilities through SIEM (Security Information and Event Management) and SOAR (Security Orchestration, Automation, and Response) solutions, creating 24x7 coverage and reducing the dwell time of criminals that manage to enter their systems.

While working with the client to establish these systems, we realised they did not have an endpoint detection & response (EDR) solution. This posed an enormous risk: endpoint devices such as phones and laptops are prime targets for cybercriminals. Yet it is very easy to overlook EDR in complex enterprises, which often assume that other security systems include EDR. But EDR is a very distinct service that can be tricky to integrate.

The Solution

Using our market-leading security services audit software, Encore, Performanta swiftly determined weak spots in the client's environment. Even though the client knew what they wanted and provided extensive information, the lack of EDR surfaced once we used Encore to get a deeper picture. We also used our assessment and gap analysis processes to spot other areas of concern or improvement.

Performanta co-developed a deployment strategy with our client, then onboarded them into the Performanta SIEM and SOAR platforms. We added critical log sources into SIEM to provide quick initial detection capabilities, deployed an EDR solution and integrated it with the SOAR solution. Our team additionally established Security Operations Centre and Incident Response processes and procedures, and established proactive threat hunting to enrich incident detection.

The Results

Our healthcare client now has comprehensive 24x7 threat detection layered across different areas, including endpoint devices. They can promptly detect security incidents, including identifying threats that may have bypassed traditional security controls. Performanta's teams and services augment their internal security teams, providing proactive threat and vulnerability detection. In addition, our client saved 17 percent on their monitoring and response costs.

Performanta's solutions have reduced the risk of dwell time (criminals lurking in the network) and insider threats. Our client has much greater visibility of their security activities. The 24x7 commitment to cybersecurity has boosted the client's confidence in its security teams and investments rattled by previous security events. Working with Performanta, they now have serious and proactive security measures in place, with the ability to continually improve their security posture through reviews and refinements.

PERFORMANTA

www.performanta.com