PERFORMANTA

Case study

Averting Disaster though Actionable Security Assessments and Integration

Leading Insurance Provider

Extended Detection & Response (XDR)

Overview

- Complex enterprise technology systems create opportunities for criminals and malicious insiders. Organisations often underestimate how many gaps and problems exist in their security environment.

- In this case study, the incoming CIO was concerned that their security provider did not provide regular incident reports.

- Performanta inspected the security services and devices with Encore, our agnostic security diagnostics platform. We deployed Encore and generated an intelligence report within a day.

- The report revealed numerous security issues, including a poorly-implemented EDR solution, a lack of active threat monitoring, and even a potential breach attempt.

- Performanta enrolled and integrated our client into our SOAR, SIEM, and SOC services.

- The client experienced a 30 percent decrease in Mean Time to Detect (MTTD) and 40 percent for Mean Time to Respond (MTTR). They now have the confidence of 24-7 automated security and usable intelligence on the state of their security.

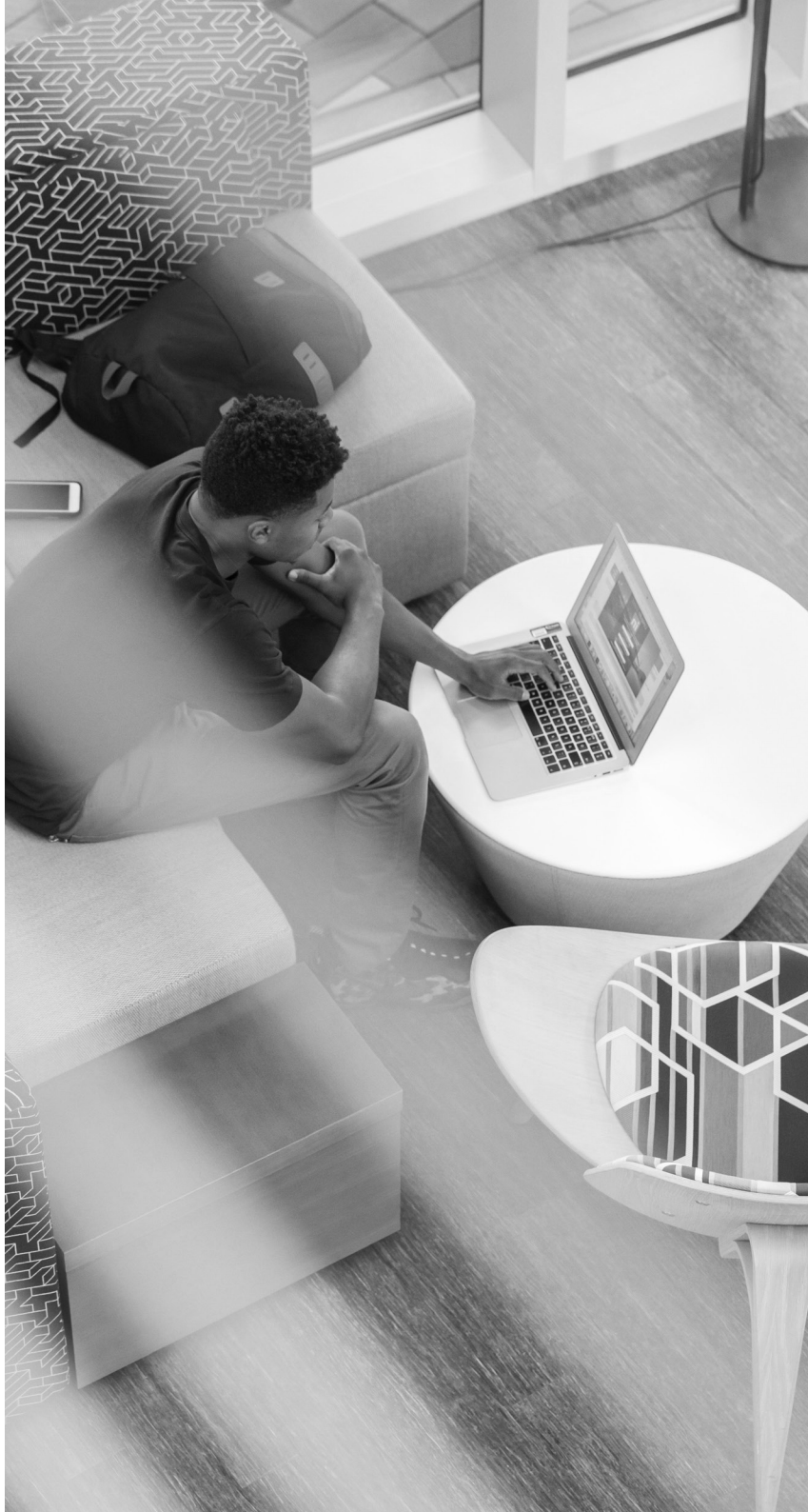
Executive Summary

The bigger they are, the more security challenges they have. This statement applies to any large enterprise's technology estate and should resonate with every CIO and CISO. Cybercriminals exploit the blind spots and gaps created by complexity—the biggest security mistake a company can make is to assume they are safe. In this case, a newly-appointed CIO did not accept the dogma. They had reason to be suspicious, such as a lack of incident reports, and they recruited Performanta to assess the environment.

We deployed our Encore platform to agnostically probe security devices and services on the network. Deploying in an hour and reporting in less than a day, Encore quickly highlighted critical security concerns. The client's established extended detection & response (EDR) solution wasn't deployed properly and only present on fewer than 60 percent of machines. There was also little regarding endpoint and device security, or threat management automation.

Using the information from Encore, Performanta and our client took steps to shore up security. We integrated the detection & response capabilities with our security information and event management (SIEM) platform, enrolled their enterprise systems onto our security orchestration, automation, and response (SOAR) platform and established 24-7 automated threat management with our security operations centre (SOC).

These changes could not have come sooner. During the project, we detected a possible breach attempt. This environment was ripe for attack, and the proactive actions of the CIO prevented disaster. Their proactive response helped bolster their standing and security's overall importance with the company's leadership. With Performanta as a partner, this regional insurance leader now owns a proactively secure and continually improving IT estate with much-reduced risks from criminals and malicious insiders.



The Challenge

A leading problem with enterprise IT estates is their inherent complexity. It can become challenging to spot problems such as misconfigurations, underreporting or blind spots. Often, it requires a new perspective to prompt questions about the estate and its security. In this case, our client has appointed a new Chief Information Officer who had previously dealt with major security incidents and wanted to test the current environment's integrity.

A specific red flag was that the incumbent security service provider had not been sending frequent incident reports. The new leader wanted to know why, also taking the opportunity to scrutinise all the security controls. This was against a strict timeline: contract renewals with the incumbent provider were approaching. The CIO needed clear intelligence quickly and affordably. Having previously worked with Performanta, they approached us to support their efforts.

The Solution

This CIO's intuition could not have been more prescient. Performanta deployed our bespoke Encore platform, which quickly probes and interrogates security services and devices on the enterprise network. Most enterprises rely on ActiveDirectory to inform their estate's security posture, but this approach often fails to cover devices such as smartphones, Linux machines, and IoT devices. Other security audit tools rely extensively on vendor agent software. Yet Encore connects directly with devices and services, sidestepping such ecosystem blind spots.

Taking less than a day to deploy and report results, Encore identified several serious issues. Our client's detection and response service was deployed on fewer than 60 percent of its machines, leading to underreporting. We also detected numerous misconfigurations that limited reporting. Crucially, we also identified a potential breach attempt in progress. With Encore's feedback, we onboarded the client to our security information and event management (SIEM) platform within a week.

The Results

Performanta quickly closed our client's security gaps. Other than properly configuring the EDM solution and onboarding the SIEM platform, we integrated the EDM with Performanta's security orchestration, automation, and response (SOAR) platform and security operations centre (SOC). These actions helped unite the client's security, deliver operational reporting, and establish continuous and automated 24-7 visibility and improvement. By effectively utilising SOAR, the client experienced a 30 percent decrease in Mean Time to Detect (MTTD) and 40 percent in Mean Time to Respond (MTTR).

The first step to action is knowledge, and with Performanta, the CIO and their team quickly saw the forest for the trees, took action, and avoided serious security incidents. They gained necessary intelligence, influencing their security strategy and avoiding costly contract renewals for underperforming services. This bolstered their standing with the company and dramatically reduced cyber risks.

PERFORMANTA

www.performanta.com