CUSTOMER CASE STUDY

How Hyde House reduced cyber risk by enabling their in-house team with security expertise and transparency

Hyde

Industry
Real Estate

Sophos Solutions
Sophos Emergency
Incident Response

SOPHOS

The challenges

- Need rapid notification and assistance when threat is discovered.
- Lack of visibility into provider's platform used for alerts and investigations.
- Inability to monitor across multiple sources (cloud, on-premise, SaaS).
- Reactive approach from previous provider.

When Mantas Marcinkevicius became IT Security Manager at Hyde Housing in 2021, one of his first priorities was to elevate the company's security maturity. Hyde Housing had previously deployed a third-party SOC service with SIEM technology that did not have visibility or access into the technology managing threat alerts and investigation. He had to email the vendor to request data for reports.

"We had a few cybersecurity events, and we really struggled with getting any visibility from the previous managed SOC provider," Marcinkevicius said. "It just didn't provide us with much value. We had to go do a lot of the work ourselves, even though we were paying for a third-party service. We were just always in a reactive mode. We needed a proactive approach with greater visibility."

When the Log4J malware was discovered in December 2021, Marcinkevicius and Information Security Analyst Rajevan Shanthakumar expected their security provider to proactively investigate and ensure Hyde Housing was not at risk. Instead, Marcinkevicius and Shanthakumar spent their holidays doing this work themselves, and the lack of visibility, transparency, and access to data proved to the company that it needed a better solution.

"It was an easy decision to seek an alternative," Marcinkevicius said. "I realized we couldn't have this service anymore."

The solution

- Immediate access to security experts via transparent Sophos Taegis platform.
- Proactive 24/7 threat detection, investigation, and response.
- Impactful threat intelligence with unmatched visibility across their threat landscape.

Marcinkevicius began the search by looking at extended detection and response (XDR) solutions that would provide visibility into the detection, investigation, and response to threats. He studied third-party research reports, attended several security conferences to explore solutions on the marketplace, read white papers, and talked to peers. Hyde Housing needed a solution that would provide visibility across their entire IT landscape as well as alert triage and escalation, investigations performed, and response action options. They also wanted the ability to tap into a deeper level of security expertise with a partner who would work closely with them on a common goal of improving security maturity.

"We had to go do a lot of the work ourselves, even though we were paying for a third-party service. We were just always in a reactive mode. We needed a proactive approach with greater visibility."

Mantas Marcinkevicius
IT Security Manager,
Hyde Housing

"We needed a solution that connected all of our disparate systems, included around-the-clock security monitoring, and one place where you can access all our data with full transparency," Marcinkevicius said. "We needed to be able to log into the same XDR platform that our MDR provider analysts do, and have this 24/7 view and unfettered access to everything."

Sophos Taegis MDR is a managed detection and response (MDR) solution that provides customers with superior detection and unmatched response around the clock. The MDR offering includes direct access to cybersecurity experts within 90 seconds, full-service incident response capabilities, one year of raw telemetry storage, impactful threat intelligence, and proactive monthly threat hunting.

The solution is delivered via the open and transparent Taegis XDR platform, which gathers and interprets telemetry from proprietary and third-party sources throughout a customer's environment, including endpoint, network, cloud, identity, OT, email, and business applications. Sophos MDR solutions combine powerful cybersecurity analytics from the Taegis XDR platform with extensive human expertise from security experts to lower customer risk and reduce the burden on a customer's security staff.

A company where Marcinkevicius previously worked used Secureworks, now a Sophos company. He had seen evidence of Sophos endpoint agents detecting threats and security analysts investigating and responding to those threats. He selected three finalists from a group of 10 solutions for proof of concepts.

"From the planning stage and how everything was done in the proof of concept, all of us had a really good impression of Sophos," Marcinkevicius said. "There was very good engagement from both the technical teams and the sales teams. It was just a really pleasant experience. Taegis scored the highest in our success criteria evaluation, and it was the best priced solution."

"Taegis is very easy to use. I really like the way the user interface is designed and how easy it is to reach out to someone from the SOC team within a few clicks on the Taegis platform. It is reassuring to have the ability to reach out to the SOC team quickly and clarify any security issues or concerns."

Rajevan Shanthakumar
Information Security Analyst, Hyde Housing

Results and impact

- Reduced risk with visibility and access to all security data.
- Realized cost savings by extending capabilities of internal team.
- Maximized value of existing IT investments with out-of-the-box integrations.

One of the important factors for Marcinkevicius in choosing the Sophos MDR solution is the wide array of available integrations. Taegis features hundreds of integrations, helping protect a customer's existing technology investments. Hyde Housing has a strong Microsoft presence and needed integrations with Office 365, Azure, and other critical technologies.

"I wanted everything included," Marcinkevicius said. "On-premise. Cloud. SaaS applications and custom integrations. Office 365, Azure, network technology. We needed a solution that could ingest telemetry from the wide variety of sources we have in our environment to help elevate our security posture."

Pulling all that data from across Hyde Housing's environment into one place provides holistic visibility and makes life easier for the company's small security team.

"Taegis is very easy to use," Shanthakumar said. "I really like the way the user interface is designed. As an example, you go to detection types and you can select stolen credentials, you click on it, and you get any alerts related to stolen credentials right there."

With Sophos MDR solutions, both Shanthakumar and Marcinkevicius benefit from from Sophos MDR's rapid responsiveness. Sophos security analysts are available via live chat in Taegis within 90 seconds and work alongside customer resources on investigations, adding security expertise to the Hyde Housing team without the company having to hire and retain additional resources.

"I really like the support I get from the security analysts in the SOC," Shanthakumar said. "It's a 10 out of 10. You know when you click on chat and ask an analyst a question that you're going to quickly get the answers needed from an experienced security expert. And the investigations by the security analysts are very good, very detailed. As soon as we see it, we know where to look and where to get started."

Added Marcinkevicius: "It's like having a senior colleague to go to and ask for help, which provides us tremendous value because we only have one in-house analyst. Sometimes things get very busy, but we always have someone watching our environment with Sophos. We also reduce costs because we do not have to try and hire and retain in-house expertise."

Looking ahead

The availability of that level of security expertise, plus impactful threat intelligence, one full year of raw telemetry, monthly threat hunts, and quarterly security reviews have helped Hyde Housing elevate its security program in a cost effective way.

"If we do have an incident, there are very capable security experts right there to jump in and help us contain the incident," Marcinkevicius said. "I have much better metrics. It's a fully transparent platform. We have instant access to experienced security experts. It's just night and day from our previous solution, and makes a really big difference for reducing our business risk."

"There was very good engagement from both the technical teams and the sales teams. It was just a really pleasant experience. Taegis scored the highest in our success criteria evaluation, and it was the best priced solution."

Mantas Marcinkevicius
IT Security Manager,
Hyde Housing

To learn more visit Sophos.com

SOPHOS