CASE STUDY

Incident Report: Remote Access Server

Cyber-attacks are commonly driven by external threat actors. However employees can unintentionally become one of the biggest threats to your organization. Most often employee intentions are good, but serious risks can arise from something as simple as clicking on a malicious link, downloading the wrong file or connecting to the wrong remote server.

When an early-stage eSentire Managed Detection and Response™ service client found themselves faced with an insider threat, they had an opportunity to experience eSentire's white glove service first hand.

Proof of Concept

At eSentire, our proof of concepts (POC) are completely customized to our clients' needs. We establish check points throughout the process to continually ensure delivery matches the client's unique cybersecurity needs. Throughout the process, we review events that our Security Operations Centre (SOC) responds to. Ten days after a POC launches, we connect with our client to walk them through the types of network events observed.

Discovery

A significant number of brute force attacks coming through remote access servers originating in Europe and South East Asia were observed by the reviewing team. This was unusual, as the client didn't have any remote access servers. It was unknown how long the remote servers were in place - it could have been weeks or even months. They continued to review additional events uncovered by the SOC, including alerts originating from a financial technology solution. This was suspicious as the client confirmed that they hadn't commissioned the solution. Both events were found by our SOC within the first ten days of the POC's life cycle.

Prevent and Protect

The analysis didn't stop with these discoveries. Upon deeper investigation, SOC analysts discovered that a support staff team had created their own IT resources not knowing that the action would make the company vulnerable to attack. Analysts worked with the client to patch this hole. Rather than finish the POC, the client enlisted Managed Detection and Response to guard them from additional exploit. Within three weeks, the SOC successfully blocked three variants of cryptolocker – three different forms of ransomware.

Cyber threats can come from inside and outside of your firm. Being able to react quickly is crucial, especially when confidential information is involved. Our 24x7 team of elite security analysts live inside our technology – monitoring, hunting, and responding to threats. Is your firm at risk? Contact us to learn more about how Managed Detection and Response can help protect your organization from cyber threats.