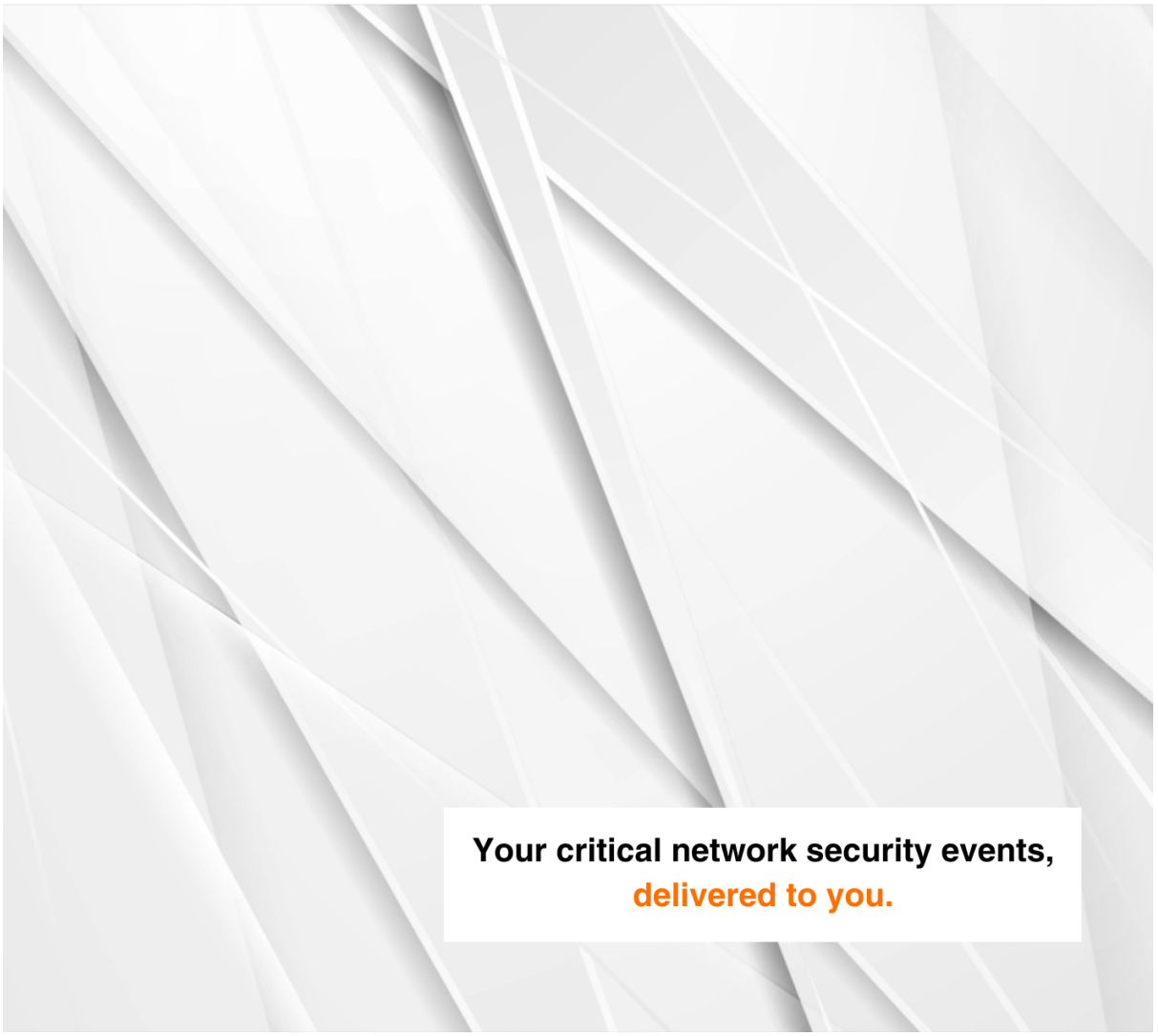
hyprfire®

Customer Story:

Protecting Local Government and Rate Payers' Data and Infrastructure from Advanced Persistent Threats (APT)



Customer Story: Protecting Local Government and Rate Payers' Data and Infrastructure from Advanced Persistent Threats (APT)

Overview

Our client is an Australian local government council that employs over 200 staff and services over 38,000 people and businesses with municipal infrastructure and services. The council also holds extensive personal and business data on its constituents within its borders.

Background

Our client's IT department had previously deployed the cyber security solution stack of Perimeter, Endpoint and Network Detection and Response (**NDR**) tools as essential defences against attackers.

Challenges

Before coming to us, our client's second-generation NDR solution had been in place for approximately 5 years.

While our client believed that the solution was doing its job, it was expensive and the large number of ticket alerts it was feeding into their HelpDesk software made it difficult for our client's team to address potential threats given their limited human resources.

Their second-gen solution had taken many months to deploy and tune to operate in the client's workflow. In addition, the NDR provider did not provide local support and support was very difficult to access generally.

Our client came to question whether they were receiving value for money from their legacy NDR solution.

Solution

Hyprfire's Firebug was configured to replace the legacy NDR solution directly. It would be deployed and managed by the customer's existing Managed Security Services Provider (**MSSP**).

At 2pm on 31 August, a Hyprfire Firebug was provided to the client’s security team effectively, and deployed by that team within 2 hours of receiving it. Once deployed, it started reporting tailored information within 24 hours.

Solution #1: Discovery of APT via SSH

Within 24 hours of deployment, the Firebug identified that a device was receiving numerous successful SSH connections originating from a variety of blacklisted IP addresses and IP addresses located in unexpected geological locations.

The Hyprfire team rapidly alerted the client of this communication and identified this as an unusual activity involving a specified client server.

Upon further investigation, the Hyprfire team was able to confirm a malicious, but unsuccessful, series of ongoing SSH brute-forcing attempts. These attempts were then later checked and confirmed by the client.

As this was the first time the client had been made aware of this activity, it seems that it was not alerted by the legacy NDR solution over the previous 5 years of deployment.

Once the threat was identified, the client immediately disabled SSH connections to the device and checked that no SSH connections had been successful.

If these ongoing SSH brute-force attempts had been allowed to continue or this particular device's SSH configuration not changed, attackers would likely have gained access to a business-critical server with legitimate credentials. For example, staff and residents' bank transfer details.

From here, attackers could pivot around the network completely unnoticed by the client or the security solutions in place, leading to ransomware, data exfiltration and other attack types.

Solution #2 - Unprotected Networks

Within days of Firebug's deployment, it had provided the client with a network diagram of the deployed network. Upon reviewing the document, the Hyprfire team realised that with the current network structure, the client had five physical sites with unmonitored network traffic.

These unmonitored devices can communicate with the internet without having their traffic observed by security solutions, allowing for potential backdoors to be accessed or malicious network scanning to occur.

In addition, one of these unmonitored sites is a disaster recovery redundancy site which, in the case of a major outage of the main admin centre, all systems would revert to this, potentially corrupted, unmonitored site.

As a legacy decision, these network changes were made as redundancy solutions while the previous NDR solution was in place and monitoring the former network. The previous NDR solution had reported no changes in the volume of traffic when the changes were being made, which would have alerted the client to the removal of monitoring caused by the change.

Looking Forward

Hyprfire demonstrated its effectiveness within 24 hours of deployment and enabled the client to identify and recover from two critical security events.

Given the speed and simplicity of deploying Hyprfire, our client is now in planning discussions to deploy Hyprfire in other network areas, to extend cyber defences to other priority digital infrastructure and valuable data repositories. In particular, our client wishes to cover the unmonitored sites mentioned above.

About Firebug

At Hyprfire we're committed to providing a simple, effective and affordable Network Detection and Response (NDR) solution.

Hyprfire's **Firebug NDR solution** gives organisations an effective alternative to the most sophisticated and expensive enterprise-level NDR products. Hyprfire's solution includes our Firebug **H-NDR solution** to provide constant monitoring of your network, together with our **Managed NDR (MNDR) offering** providing you with the core elements of complete network visibility and threat intelligence.

Want to see if Firebug would work for your organisation's network needs? Speak to our Sales Team today at sales@hyprfire.com.