USE CASE

How to Gain Full Visibility during an Instant Response Data Breach

Industry: Healthcare

Issue:

An incident response firm was engaged to contain a breach on a large healthcare facility's network.

Situation:

A complicated network environment stacked with legacy equipment, a basic onsite IT staff and an underperforming MSSP. Networks seem to work great when there is nothing wrong but issues are quickly exposed during attacks, as they were in this scenario. Once they were under attack, it became apparent that the network was not set up properly. The existing switches didn't have the proper firmware, they weren't configured correctly and had ingress / egress set up issues.

Challenge:

The first challenge was gaining visibility to monitor the network traffic: understand where the attackers were coming from, where they might be touching internally, and how to stop them. "We're under attack and every minute that we don't have visibility, is another minute that bad guys are exfiltrating sensitive data."

The second challenge was finding the right vendor to provide that access and visibility. "Before we found Garland our options were limited. It's either we go to a huge provider like Gigamon, which is super expensive, and doesn't give you a custom solution. Or the other end of the spectrum would be buying a 1G consumer grade mirror on Amazon and that wasn't going to solve our problem."

> **"We're under attack and every minute that we don't have visibility, is another minute that bad guys are exfiltrating sensitive data."**
>
> -Lou Rabon, Founder / CEO,
> Cyber Defense Group

This document is for informational purposes only. The information in this document, believed by Garland Technology to be accurate as of the date of publication, is subject to change without notice. Garland Technology assumes no responsibility for any errors or omissions in this document and shall have no obligation to you as a result of having made this document available to you or based upon the information it contains.

USE CASE

CDG
Cyber Defense Group

GARLAND TECHNOLOGY
See every bit, byte, and packet

How to Gain Full Visibility during an Instant Response Data Breach

Industry: Healthcare

Result:

"When I found Garland, I got a network expert on the phone and they configured a custom solution for us. Once we got the TAPs on site, I found out how configurable they were and how simple it was. Really from the beginning, from sales to the solution, to support, was great. I can't say enough good things."

Solution:
Cyber Defense Group utilizes two Garland Technology 'Breakout' TAPs and one Bypass TAP, in aggregation mode to feed proprietary tools they use for full packet capture in the cloud, intrusion detection, enterprise security monitoring, NGFW and log management. "We were able to get the visibility we needed quickly. That allowed us to do what we needed to do to find the bad guys and kick them out."

Note: 'Breakout' mode sends each side of traffic to separate monitoring ports. Ensuring that no packet is lost to high-priority monitoring tools. Aggregation mode merges traffic streams into one monitoring port to reduce appliance costs, often used in combination with filtering taps, ie: filter, aggregate data streams.

Tools Deployed:
2x Garland Technology's P1GCCB Copper TAP
1x Garland Technology's P1GCCBP Bypass TAP
Cyber Defense Group / proprietary tools

> "When I found Garland, I got a network expert on the phone and they configured a custom solution for us. Really from the beginning, from sales to the solution, to support. I can't say enough good things."
>
> -Lou Rabon, Founder / CEO,
> Cyber Defense Group

This document is for informational purposes only. The information in this document, believed by Garland Technology to be accurate as of the date of publication, is subject to change without notice. Garland Technology assumes no responsibility for any errors or omissions in this document and shall have no obligation to you as a result of having made this document available to you or based upon the information it contains. ©2018 Garland Technology LLC. All Rights Reserved