Incident Response

Proposition Overview

Security breaches will occur, the only variable factors are timing, severity and how quickly you can respond

From ransomware attacks with the potential to cripple back-office operations and expose patient data, to more sinister 'killware' that can compromise vital healthcare equipment – and in turn patients – the past two years have introduced a wave of new threats that healthcare providers must address. As threats actors evolve their Tactics, Techniques and Procedures (TTPs), your organisation's preparedness should evolve too, when your organisation faces a severe cyber incident, will you be ready?

At a glance

- ✓ We'll work with you to make sure threats are quickly contained with rapid deployment and investigations.
- ✓ We'll stand side by side with your teams to eliminate threats with the help of our industry-leading security tools.
- ✓ We'll help you to recover, restoring business as usual operations quickly, and with as little disruption as possible.
- ✓ We'll learn from the incident, suing digital forensics to understand root cause and prevent recurrence.

Problem solved

By providing an incident response service in addition to threat detection, we reduce security team handover delays and speed up the SOC's "time to effectiveness". This means the time between a data breach being detected, and when a team is primed to act effectively as an incident responder, is reduced. This is critical in the early stages of a data breach, when time is often lost because applications are incompatible, or teams fail to communicate the information as quickly or efficiently as machines can.

Benefits

Backed by Unit 42, giving access to one of the world's largest and most experienced threat intelligence teams.

An experienced team of security consultants with backgrounds in public and private sectors.

Leverage industry-leading tools to jump start your investigation enabling you to get back to work, fast.