Local Government needed to understand the impact of a suspected ongoing breach. What was the scope of the breach? What type of data was stolen (i.e. PII, PHI, Financial, etc.)? Has the breach been contained? Do they need to report the breach? Is a breach notification required?

They didn’t have a security team or tools in place to investigate or respond to the breach. The local government system did not have adequate audit records or configurations to be able to investigate the breach. They were not prepared as many organizations are not prepared.

“InfusionPoints rapidly responded to our incident and helped us contain a serious breach. The breach started with a malware infection from a phishing attacked. We thought we removed the threat. However, we started to see attacks on many of our servers and client systems. We were playing whack-a-mole. InfusionPoints, jumped in right away took control of the situation and immediately we started seeing result” Director Public Service

Rapidly responded to an active breach

InfusionPoints rapidly responded to an active breach in progress by quickly discovering how the breach started, and what the was the scope of the breach by combining three of InfusionPoints VNSOC360 capabilities;

- VNSOC360° Incident Response capability we quickly identified the indicators of compromise (IOCs), and systems and accounts that were compromised. Which allowed us to scope the breach and identify the lines of communications and notifications that were required. In parallel, begin to contain and eradicate the threat.

Key Results

- Eliminated Active Breach
- Assisted with notifications and communications
- Assisted with state investigators
- Better prepared when the next breach occurs
- Added team of VNSOC360° Cyber Security Experts to their team
• VNSOC360° Monitoring and Logging capability that includes: threat intelligence, network and host intrusion detection, security information and event management (SIEM), vulnerability, log, asset, and availability management, this solution was added to their environment to improve visibility into their environment and to ensure the remediation efforts were working.

• VNSOC360° Digital Forensics Identify & evaluate exposure, data acquisition, data analysis, and forensic examination and reporting, this allowed us to leverage our process, tools and facility to quickly develop the necessary reports for legal action.

We supported them from our InfusionPoints’ Cyber Security Center, staffed 24 hours a day, 7 days a week and 365 days a year.

“InfusionPoints’ team jumped right in and provided rapid turn around for the breach investigation.”
-- County IT Director

Supporting our customers at every step of the way during an active data breach

By utilizing InfusionPoints’ cyber security subject matter experts, and VNSOC360° to stop the active breach, investigated the incident, documented the breach and provided future protection with active monitoring of their IT environment.

This breach investigation and solution has also brought this local government peace of mind, knowing that VNSOC360° is proactively providing an early warning system for things that go bump in the middle of the night.