Right now, end-users are under attack, 93% of all successful cyber attacks start with a phishing email. Hackers and threat groups target end-users on the network to gain a foothold and, from there, use several tactics and techniques to maintain persistence and spread across the network. The Election Department currently uses antivirus (AV) to protect election computers, which uses signatures to identify known viruses/malware. AV provides a valid and useful service; however, hackers and threat groups are continually modifying their malware, so AV providers are always playing catchup. The hacker's toolset includes built-in windows applications, fileless attacks, and many more that traditional AV doesn't detect.

This means the Election Department is left vulnerable and unable to detect most current threats. They are not just at risk to advanced groups that use zero-day exploits. Without better detection, the Election Department is at risk of being compromised by commodity malware easily accessible on the internet.

Managed detection and response (MDR) services fill this cybersecurity gap. MDR is a 24/7 threat monitoring, detection, incident analysis, and response service that correlates specific threat intelligence and telemetry collected from the Election Department's environment. MDR utilizes endpoint detection and response (EDR) client software as well as network and threat intelligence to facilitate effective outcomes. Combining improved detection with a 24/7 security operations center (SOC) to monitor and respond to threats, MDR services will significantly improve the security posture of the Elections Department.