Steps Taken to Strengthen Cybersecurity Across the Public Healthcare System

IHiS
Because IT's in Healthcare

With heightened cybersecurity threats, IHiS has taken active steps to strengthen cybersecurity across the public healthcare system. As cyber threats become increasingly advanced, sophisticated, and persistent, IHiS has identified and initiated further measures that are being implemented progressively.

01 PREVENT

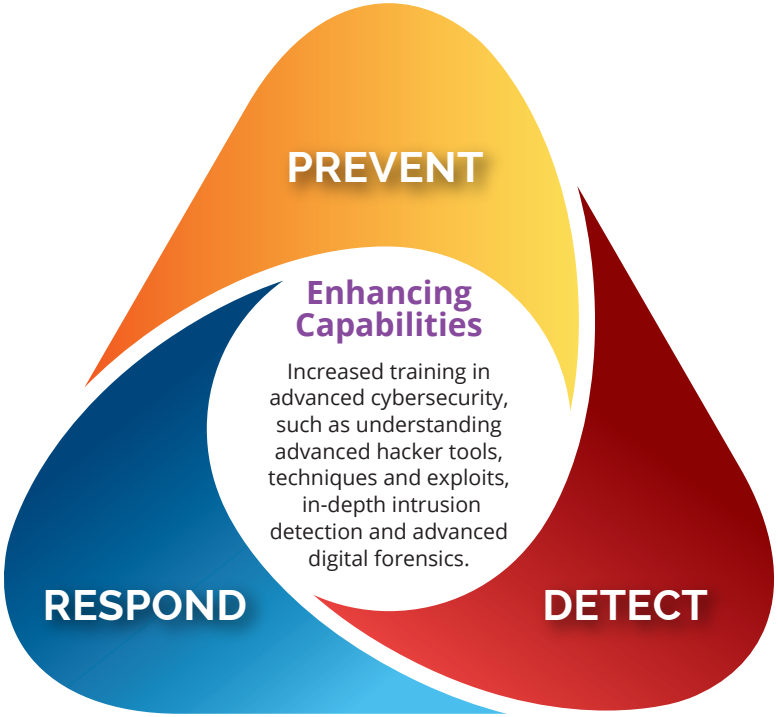
Client Advanced Threat Protection
Block threats based on exploit techniques and sophiscated malwares used by advanced threat actors

Temporary Internet Surfing Separation
Machines connected to the internal network are not allowed to access the internet

Advanced Authentication
- Two-factor authentication for local administrators managing end-user devices and software installation
- Complex passwords managed centrally with automated updates and protection of accounts

Access Restriction
Enhanced access control to allow only authorised devices that are patched with updated anti-virus and anti-malware signatures to connect to the network

Virtual Browser
Pilot of solution where users can only access reproduced content on the web to minimise risks of downloading and executing malicious files which may reside on the original sites



02 DETECT

Detection of Threats
Address advanced persistent threats by improving ability to detect indicators-of-compromise, record and monitor endpoints' system-level behaviours and events, detect advanced malwares and remove the threats, if any

Threat Hunting
Where proactive and iterative searches are conducted to detect malicious or suspicious activities

Threat Analytics
For earlier detection of suspicious account activities by applying a combination of statistical modelling, machine learning, as well as behaviour analytics to identify unusual activities

Database Activity Monitoring
Enhanced monitoring to include more comprehensive blocks and alerts on bulk queries

03 RESPOND

Advanced Security Operations Centre
Expanded suite of advanced cybersecurity services that include threat intelligence, response and remediation measures to abnormal activities and potential threats

Tightened Process
- Suspicious IT incidents to be reported within 24 hours, even if initial investigations cannot determine that they are security incidents
- Additional checklists to be put in place to ensure compliance with the SOPs