jos

Asia's Top Cybersecurity Risks

Defend with Threat Hunting

jos

Threat hunting is an active defence strategy that uses automation and threat intelligence analysis to detect and identify threats

How does it work?

Data collection

Proactively search and identify suspicious activity data

Analysis

Analyse internal data and threat intelligence with external intel to establish attack hypothesis

Hypothesis and hunt

Use automation and machine assistance to analyse data and confirm hypothesis.
If hypothesis is not proved, return to analysis

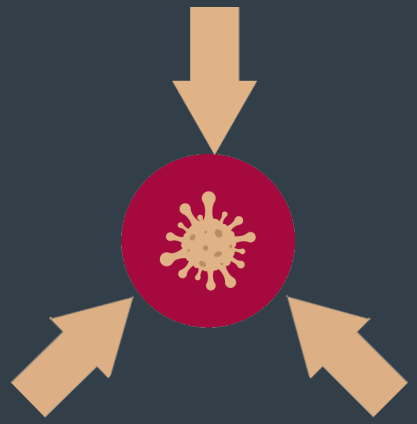
Identify

If hypothesis is confirmed, further assess the scope and impact of attack to determine response plan

Why implement threat hunting?

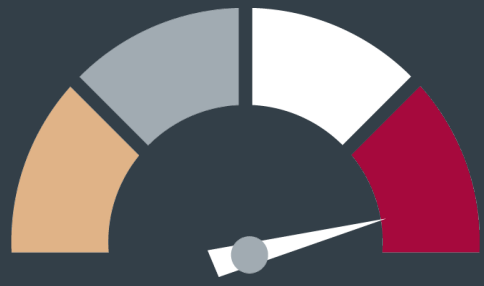
Shorten time to containment

Reduce time taken to detect and contain threats from spreading



Shorten time to containment

Reduce time taken to detect and contain threats from spreading



Shorten time to containment

Reduce time taken to detect and contain threats from spreading

Upon threat detection...

Managed Detection and Response (MDR) service providers can

Assess impact and assure business is not compromised

Conduct investigation within hours or minutes to determine response strategy

Stop the attack and restore affected files with the help of incident response experts

Investigate further to identify the source and suggest steps to avoid future attacks

jos

To learn more about Threat Hunting and MDR services at JOS,
contact us: connect@jos.com