

# 10 PROACTIVE STRATEGIES TO IMPLEMENT NOW TO DEFEND AGAINST RANSOMWARE AND MALWARE

#1

## GET FAMILIAR WITH YOUR ASSETS

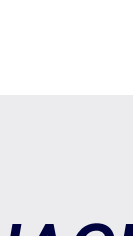
BUILD AN INVENTORY OF NETWORKED ASSETS



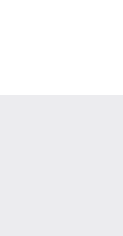
Server



Storage



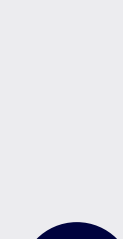
Data



Applications



Network Gear



Endpoints

#2

## CONTINUOUSLY MANAGE YOUR VULNERABILITIES



Identify Vulnerability



Analyze & Assess



Verify



Remediate

#3

## REDUCE THE ATTACK SURFACE



#4

## FIND AND BACK UP ALL IMPORTANT DATA



#5

## EMBRACE A ZERO TRUST ARCHITECTURE

Here Are a Few Tips



Audit the number of privileged user or service accounts in your domain or forest.

Example: How many domain admins and enterprise admins do you have? How many are service accounts?



Use privileged account security software.

Example: A password vault for enterprise password management.



Consider implementing AI-based continuous authentication of user accounts.

Example: Use passive biometrics (such as typing, mouse movement, gait) to continuously prove user identity.

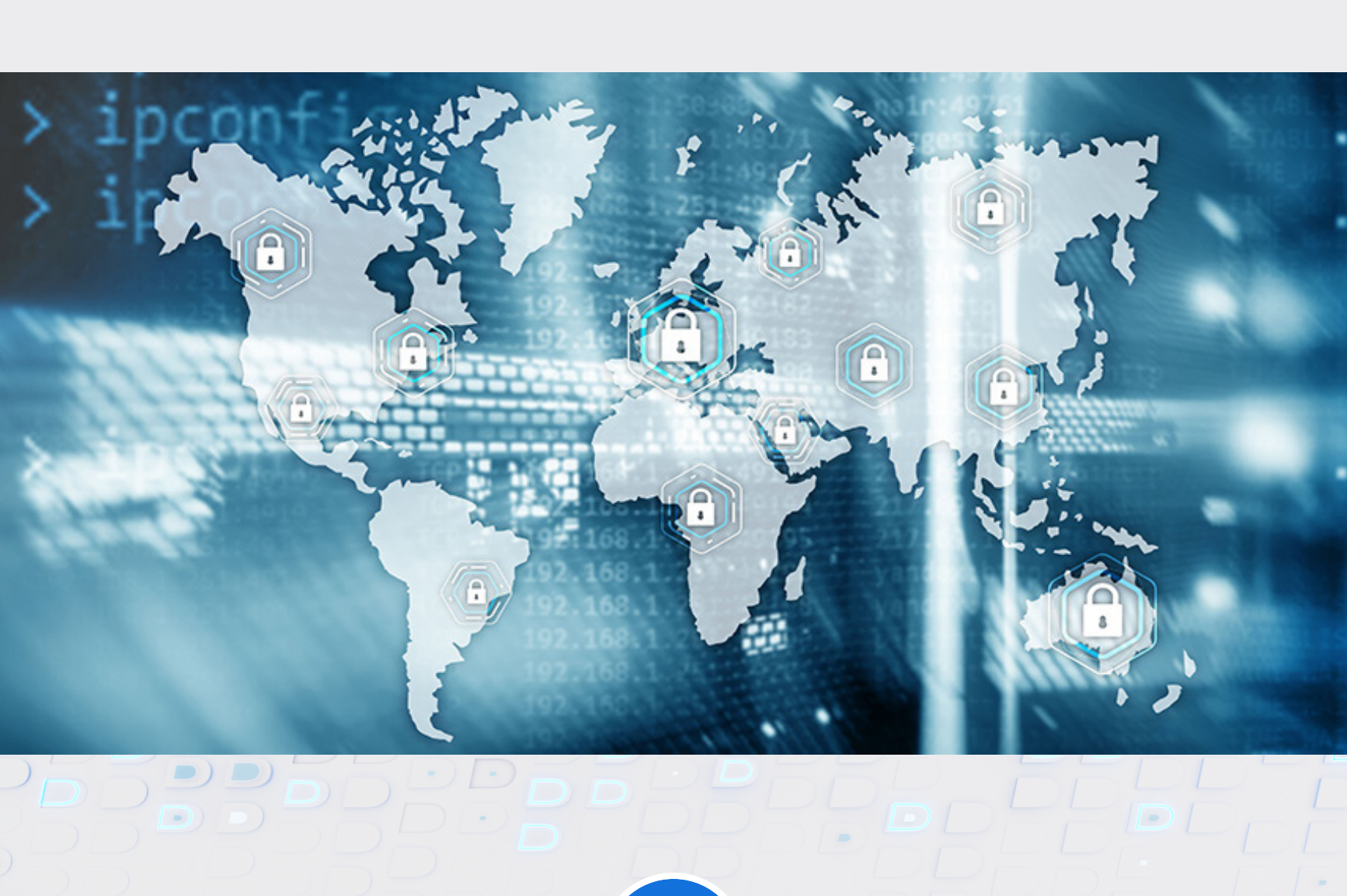


Conduct a proper red team assessment.

Example: Bloodhound and variants are effective in sniffing out privileged access violations.

#6

## BEGIN SEGMENTING YOUR NETWORKS



#7

## ENFORCE MULTI-FACTOR AUTHENTICATION (MFA)



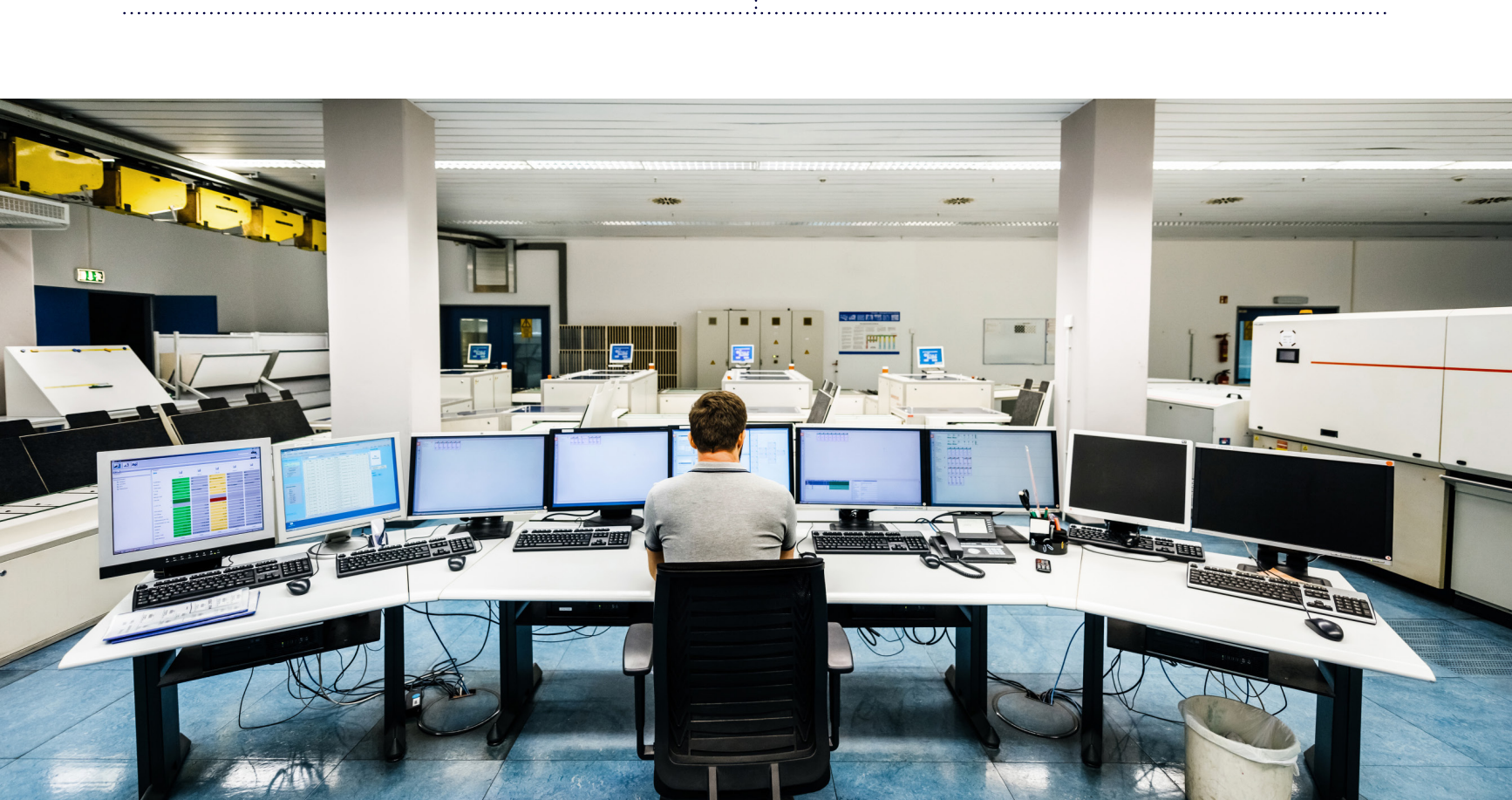
#8

## TRAIN EMPLOYEES TO SPOT PHISHING ATTACKS, BUT PLAN FOR ACCIDENTS



#9

## EMBRACE PROACTIVE MONITORING, THREAT HUNTING AND INCIDENT RESPONSE



#10

## LEVERAGE ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING



[READ THE REPORT](#) →