

IMPROVE YOUR SECURITY POSTURE A RED TEAM PERSPECTIVE

TIM MEDIN
tim@redsiege.com

BE LAZY

NOT APT JUST
PT

EQUIFAX

CIS CONTROL 1

& 2

INVENTORY

PHISHING 101

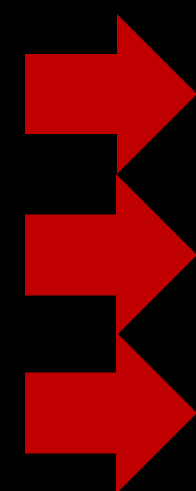
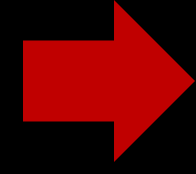
WEB FILTER

UNKNOWN

NEW

UNCATEGORIZED

FINDING A
DOMAIN



STOP
ATTACHMENTS

DISABLE

MANAGE

WINDOWS
DEFENDER

PREVENTION
FAILS

SIGNATURES FAIL

DETECTION IS A
MUST

POWERSHELL

CONSTRAINED
LANGUAGE
MODE &
LOGGING

SPECTER
MELTDOWN

BAD

PASSWORDS

PASSWORD
SPRAY

DETECT SPRAY

MICROSOFT

AZURE

2FA

2FA IS NOT
PERFECT

BEWARE OF
CRED SNIPER

THE MYTH OF ESCALATION

DOMAIN
ADMIN

IS ONLY A TOOL

KEEP IT
SIMPLE

PROTECT

DETECT



Tim Medin

tim@redsiege.com

[@TimMedin](#)

[@RedSiegeInfoSec](#)