TEXAS RE

MOVEit Vulnerability

John Romero
CIP Cyber and Physical Security Analyst

May 2, 2024

Antitrust Admonition

Texas Reliability Entity, Inc. (Texas RE) strictly prohibits persons participating in Texas RE activities from using their participation as a forum for engaging in practices or communications that violate antitrust laws. Texas RE has approved antitrust guidelines available on its website. If you believe that antitrust laws have been violated at a Texas RE meeting, or if you have any questions about the antitrust guidelines, please contact the Texas RE General Counsel.

Notice of this meeting was posted on the Texas RE website and this meeting is being held in public. Participants should keep in mind that the listening audience may include members of the press, representatives from various governmental authorities, and industry stakeholders.

Upcoming Texas RE Events

May 15, 2024

Quarterly MRC, AGR&F, and Board Meetings

May 21, 2024

Summer Outlook

May 22, 2024

IBR Registration

Upcoming ERO Enterprise Events

May 14-16, 2024

Physical Security Workshop

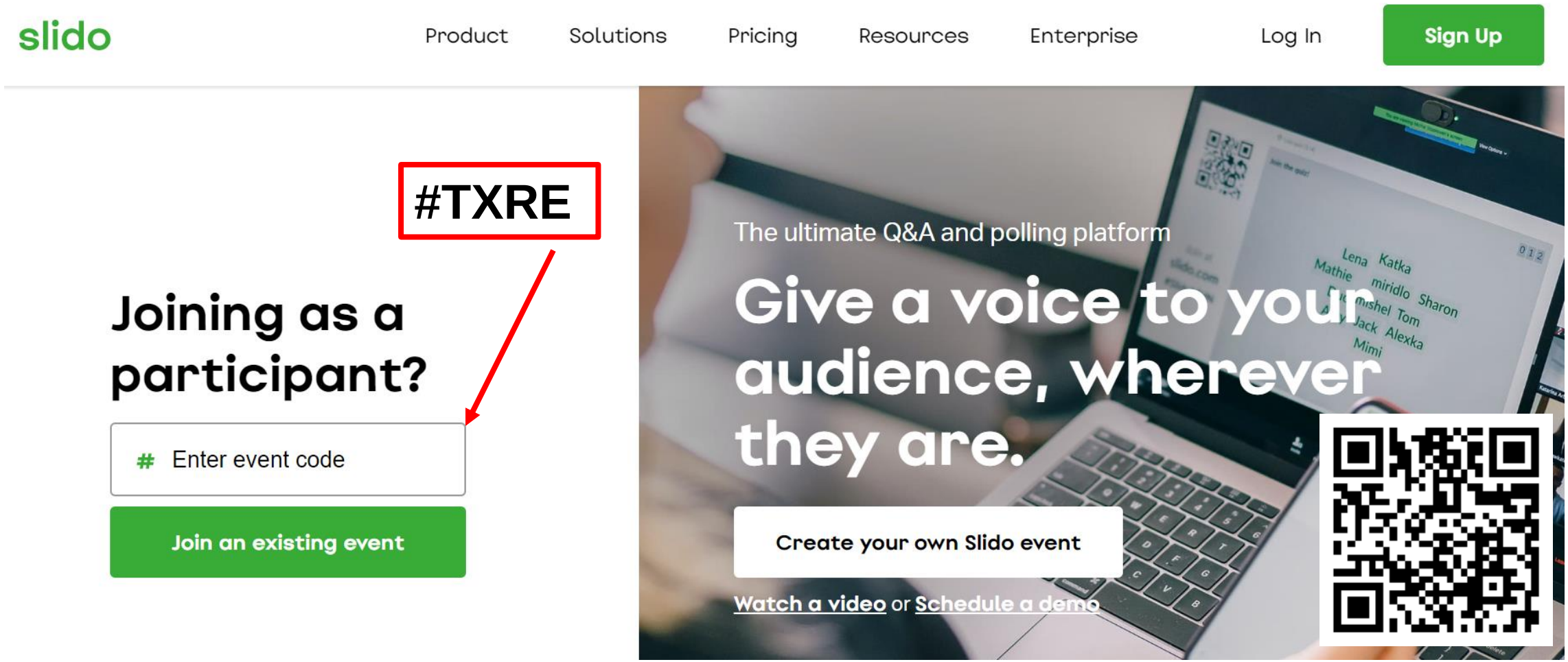
May 15, 2024

MRO Reliability Conference

May 20, 2024

Technical Talk with RF

Sli.do


slido
Product
Solutions
Pricing
Resources
Enterprise
Log In
Sign Up
#TXRE
Joining as a participant?
Enter event code
Join an existing event
The ultimate Q&A and polling platform
Give a voice to your audience, wherever they are.
Create your own Slido event
Watch a video or Schedule a demo

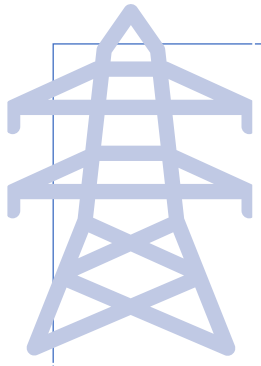
Agenda

- Why is This Important?
- What is MOVEit?
- Cybersecurity Bulletin
- Final Thoughts

Why is This Important?

Security Awareness

- Minimizes risk of incidents
- Empowers staff to recognize and mitigate cyber risks
- Cybersecurity mindset
- Compliance



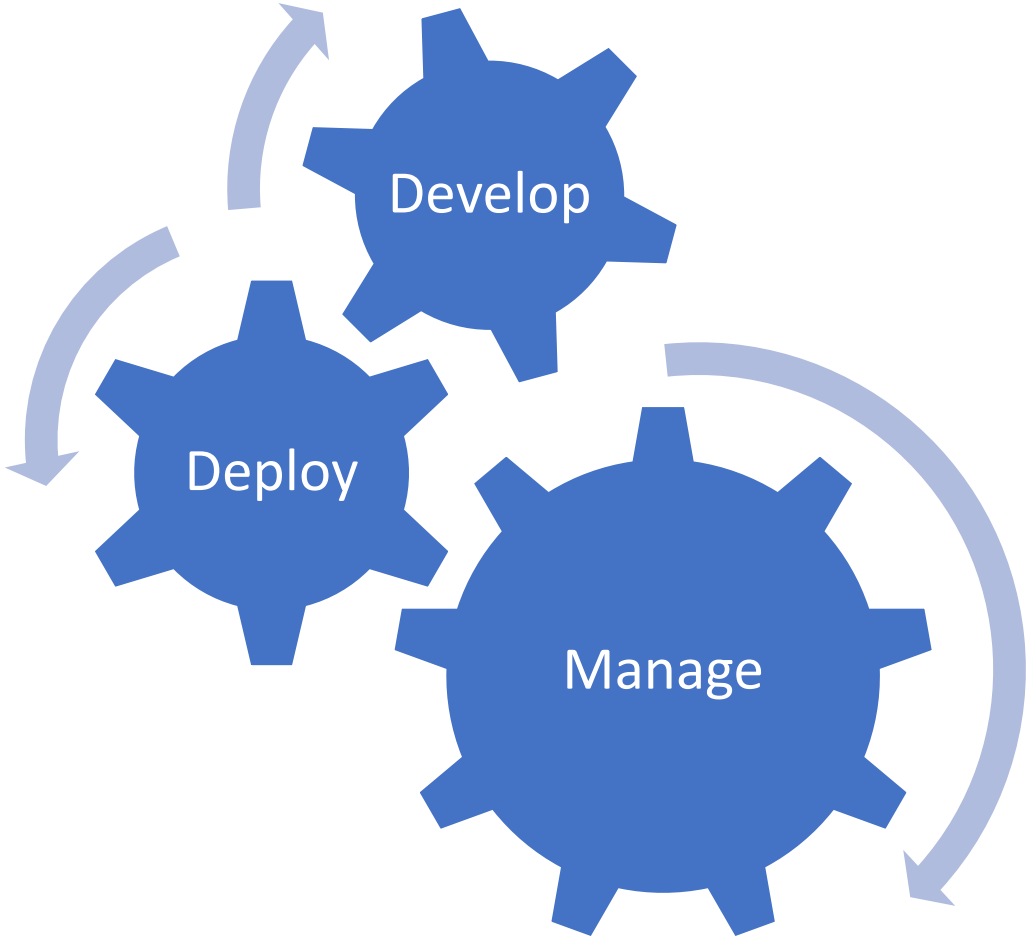
North American Electric Reliability Corporation (NERC)
Critical Infrastructure Protection (CIP)

- Mission to the Bulk Electric System (BES)
- NERC CIP Reliability Standards

What is MOVEit?

MFT: Managed File Transfer

Progress Software Corporation (Progress)



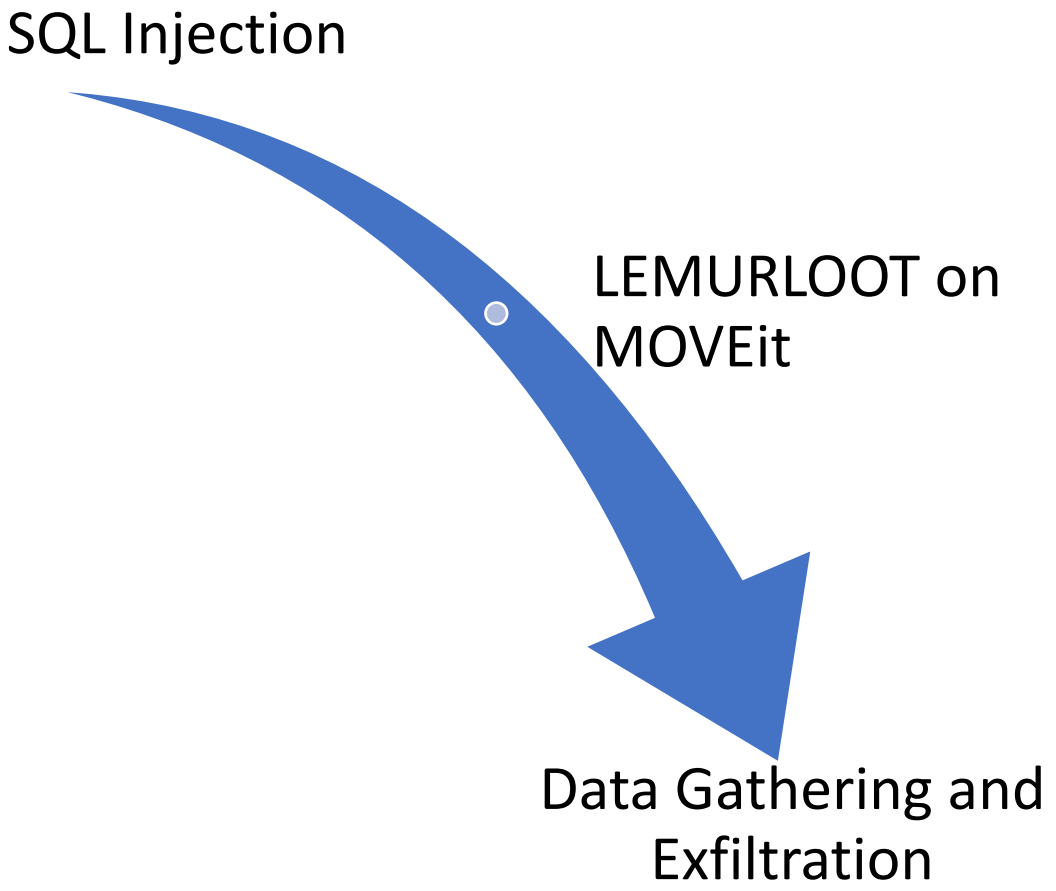
MOVEit Breach

May 31, 2023

- Initially reported

Intelligence

- Zero-day vulnerability
  - (CVE-2023-34362)
  - Web shell – LEMURLOOT
  - FlawedAmmyy (RAT)
  - Exfiltrate – C2
  - Clop



National Institute of Standards and Technology (NIST) – National Vulnerability Database (NVD)

CVE-2023-34362 Detail

Severity CVSS Version 3.x | CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NIST: NVD **Base Score:** 9.8 CRITICAL **Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

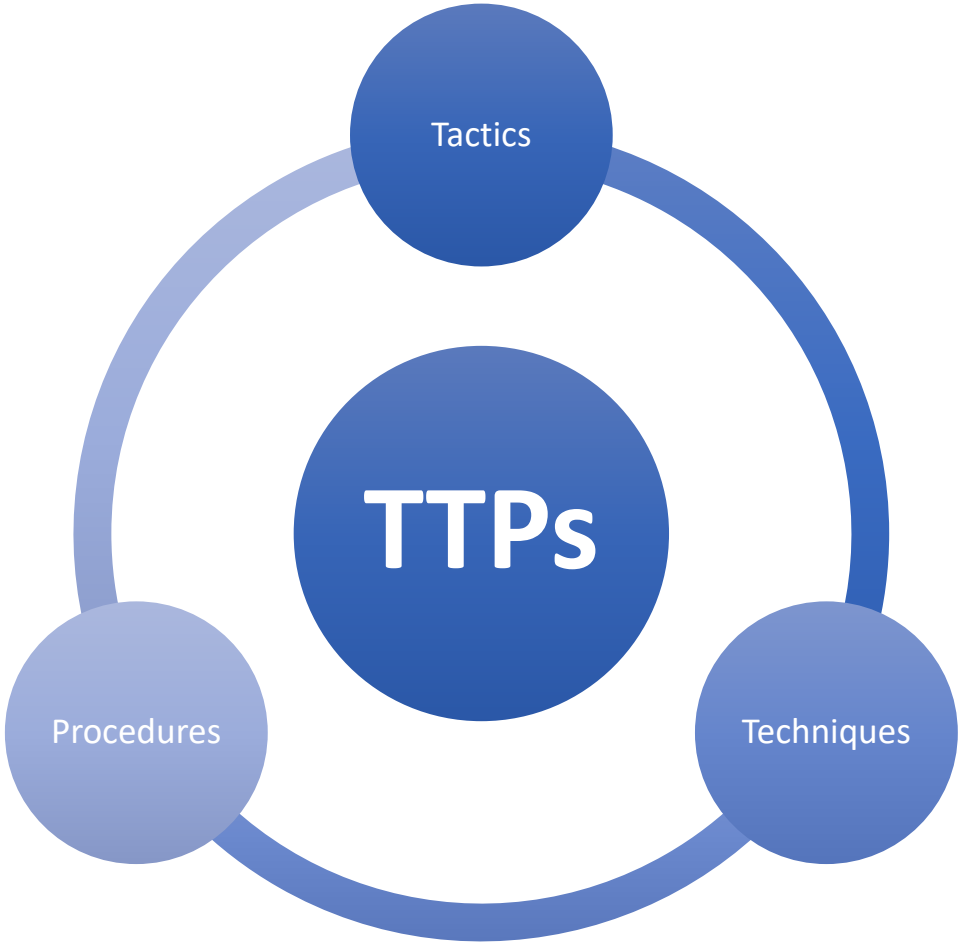
Sli.do (#TXRE)

Slido Question

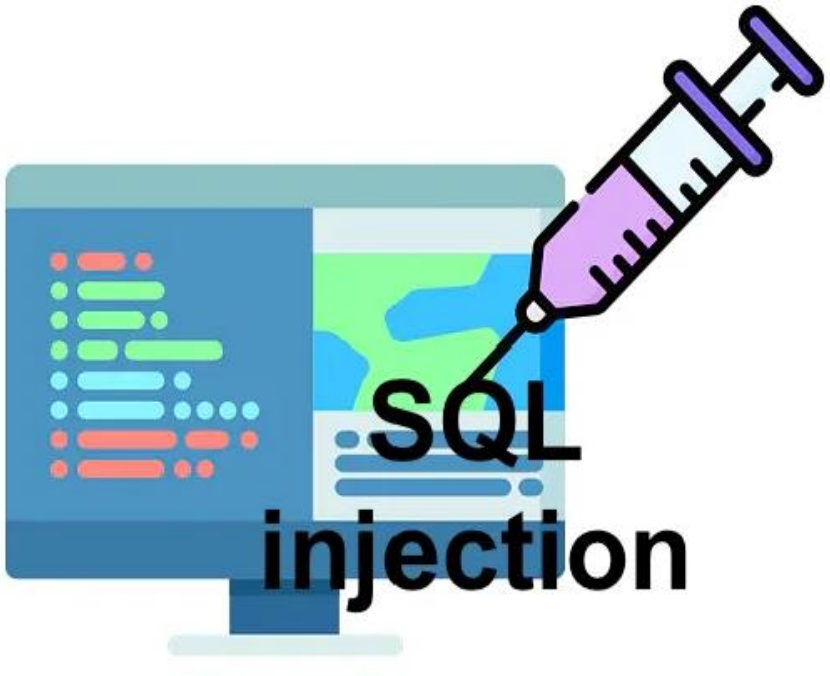
The MOVEit vulnerability has an NVD Base Score of 9.8 out of:

A. 10
B. 20
C. 50
D. 100

Tactics, Techniques, & Procedures (TTPs)



Structured Query Language Injection (SQLi)



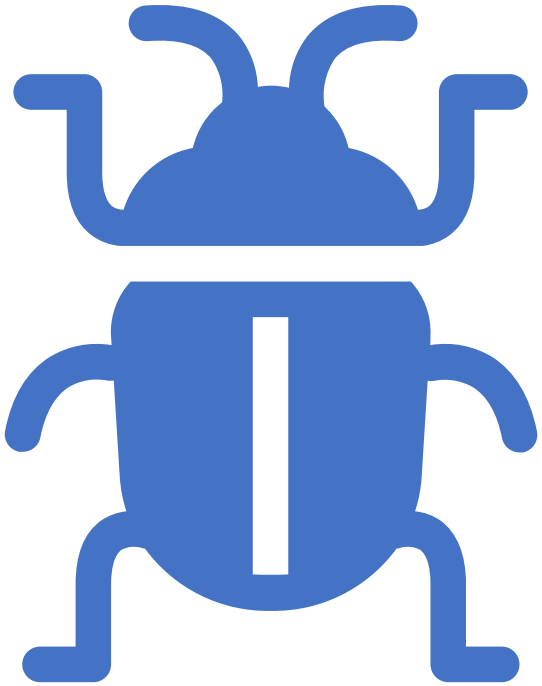
INTERNAL CONTROLS & MITIGATIONS

- Fuzzing
- Update and Patch
- Account Privilege
- Network Segmentation
- Database Accounts
- User Input Validation / Error Reporting

Cyberthreat Actors

CL0P:

- APT = TA505
  - CL0P Ransomware Gang
- Russian-speaking ransomware gang
- Clop = Klop = Bedbug



NERC CIP Standards

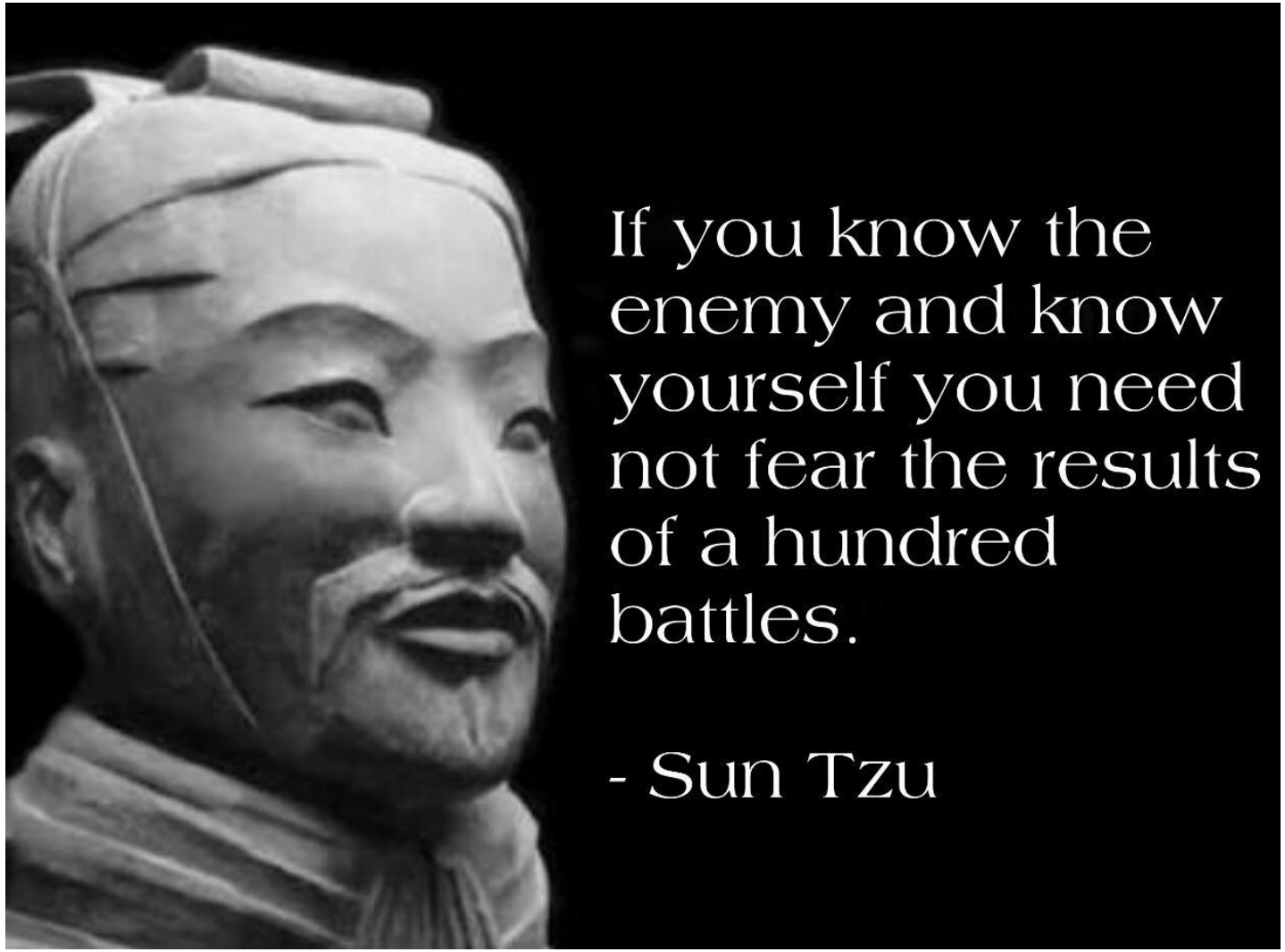
CIP-007-6

- Patch management
- Evaluation
- Mitigation

CIP-005-7

- Identification
- Monitor
- Perimeter

Final Thoughts



TEXAS RE
Ensuring electric reliability for Texans