Determining Evil from Benign in the Normally Abnormal World of InfoSec

Rick McElroy Principal Security Strategist
@infosecrick

vmware | Carbon Black.

Know normal.

Find evil.

vmware® | Carbon Black.

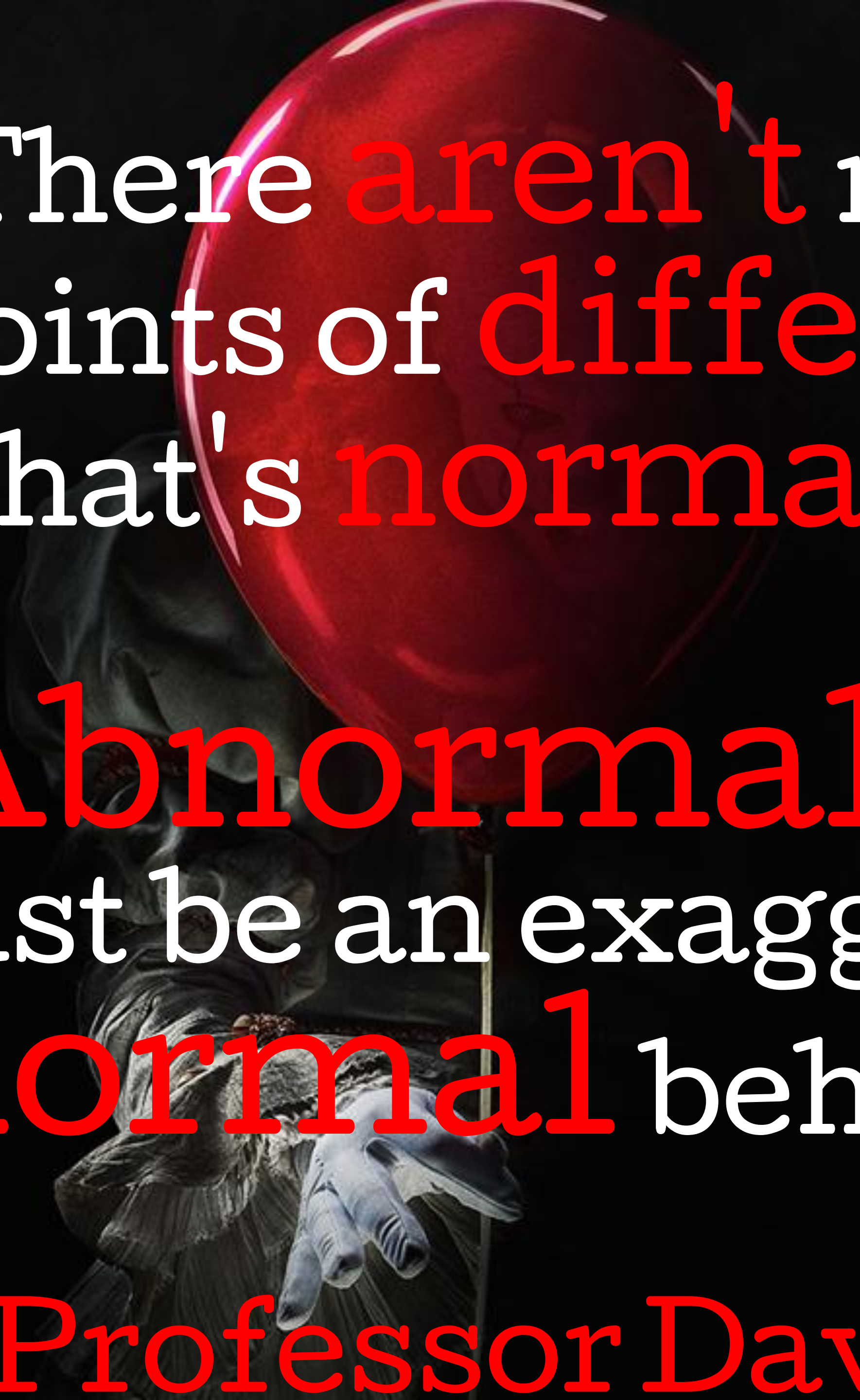
VISION

A World Safe from Cyber Attacks

NORMAL

ABNORM
AL

MITRE
ATT&CK™



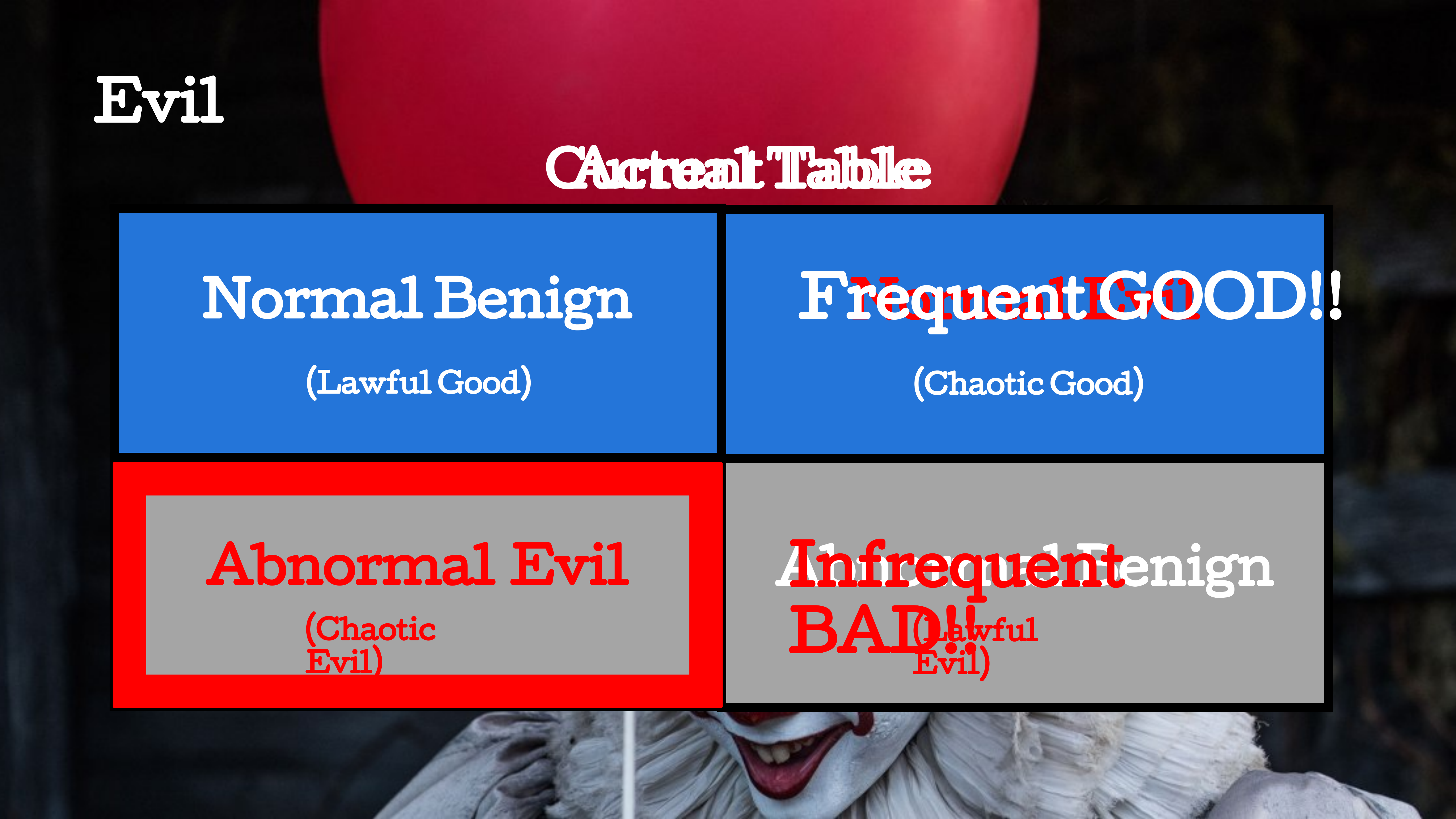
"There aren't necessarily clear points of difference between what's normal and abnormal.

Abnormal behavior may just be an exaggeration of normal behavior."

- Professor David Watson

Levels of Abnorm

- Process
- Memory
- System
- User
- Team
- Department
- Company
- Industry
- Country
- Global



Evil

Cereal Table
Actual Table

Normal Benign (Lawful Good)	Normal Evil Frequent GOOD!! (Chaotic Good)
Abnormal Evil (Chaotic Evil)	Abnormal Benign Infrequent BAD!! (Lawful Evil)

Evil..or not Evil?

Evil..or not Evil?

No enign	Normal Evil
Abnormal Evil	Abnormal Benign

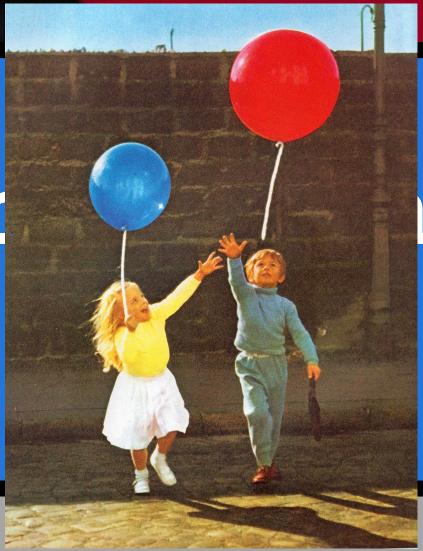
Evil..or not Evil?

Normal Benign	Normal Evil
Ab vil	Abnormal Benign

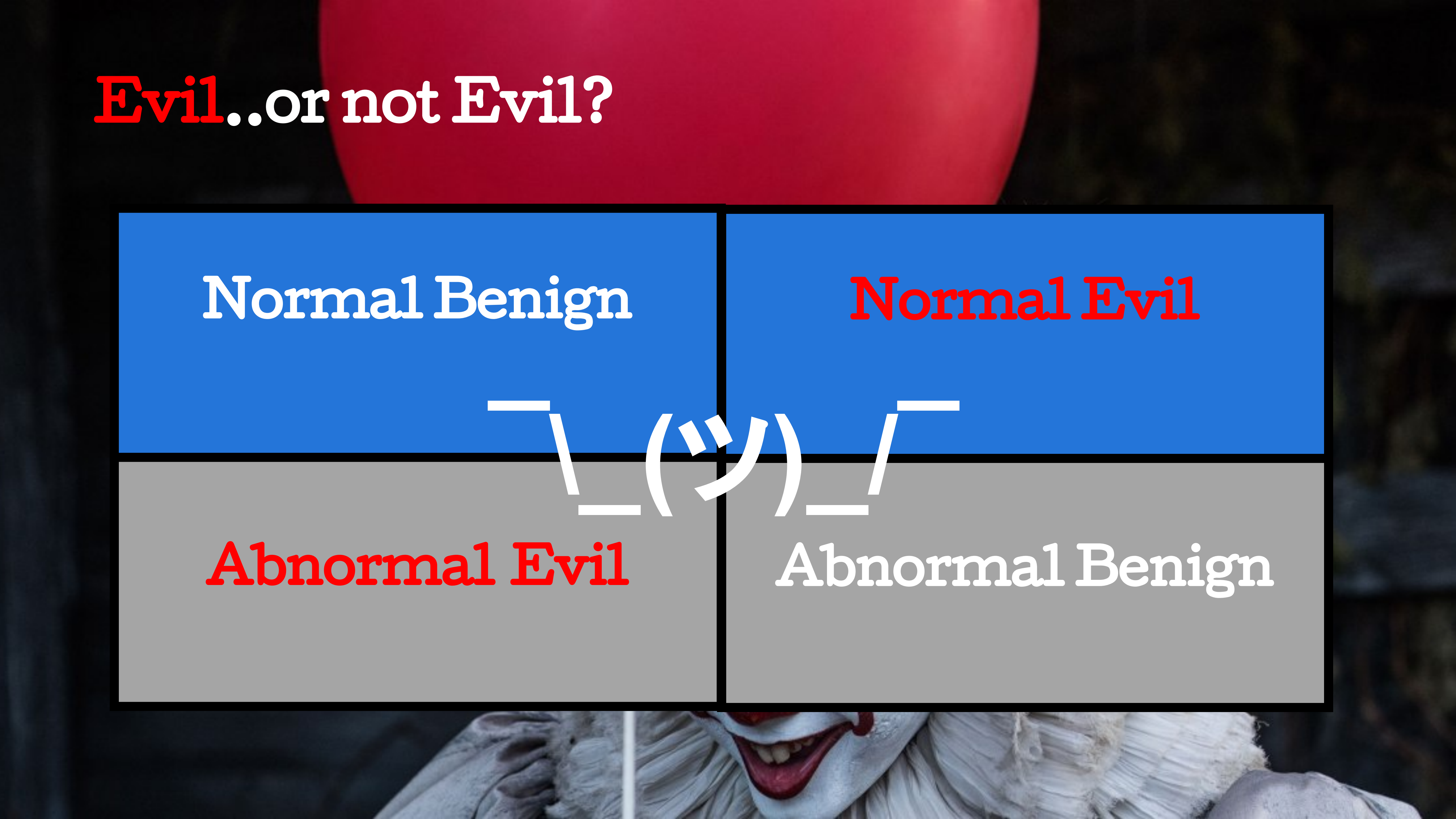
Evil..or not Evil?

Normal Benign	Normal Evil
Abnormal Evil	Abn ign

Evil..or not Evil?



Nor ign	Normal Evil
Abnormal Evil	Abnormal Benign



Evil..or not Evil?

Normal Benign	Normal Evil
Abnormal Evil	Abnormal Benign

¯_(ツ)_/¯

Know normal.

Find evil.

Carbon Black.

UNNECESSARY
NOISE
PROHIBITED
POLICE DEPT

Find Evil Faster

Contribute data back to MITRE

Share NORMINT

Help teach developers to do the right thing

Reduce false positives for everyone

Acknowledge your good fortune by shari
IT.

Stephen King

TIME
STEPHEN KING

UNNECESSARY
NOISE
PROHIBITED
POLICE DEPT

Know normal.

Find evil.

Carbon Black.

Question s?

Rick McElroy
Principal Security Strategist
@infosecrick

vmware | Carbon Black.

“We cannot change the cards we are dealt, just how we play the hand.”

— Randy Pausch