

# Determining **Evil** from Benign in the Normally **Abnormal** World of InfoSec

Rick McElroy Principal Security Strategist  
@infosecrick

An aerial photograph of a town. In the background, a large church with a tall steeple sits atop a green hill. The town below is filled with various buildings, including a prominent red brick building with a large mural that says 'DERRY'. A street runs through the center of the town, with cars visible. The sky is clear and blue.

Know normal.

Find  
evil.

Carbon Black.

vmware® | Carbon Black.

VISION

A World Safe  
from Cyber Attacks



NORMAL

ABNORM  
AL



MITRE  
ATT&CK™



A person wearing a dark suit and white gloves is holding a large, shiny red balloon. The background is dark and textured.

"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

## Cartoon Table

Normal Benign

(Lawful Good)

Frequent ~~Normal~~ GOOD!!

(Chaotic Good)

Abnormal Evil

(Chaotic  
Evil)

Infrequent Benign

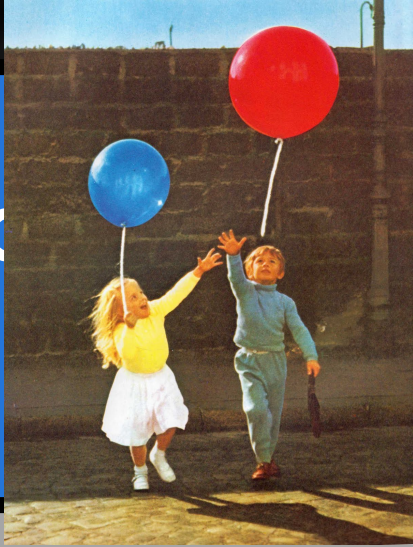
~~BAD!!~~  
(Lawful  
Evil)



Evil..or not  
Evil?



# Evil..or not Evil?



No

benign

Normal Evil

Abnormal Evil

Abnormal Benign



# Evil..or not Evil?

Normal Benign

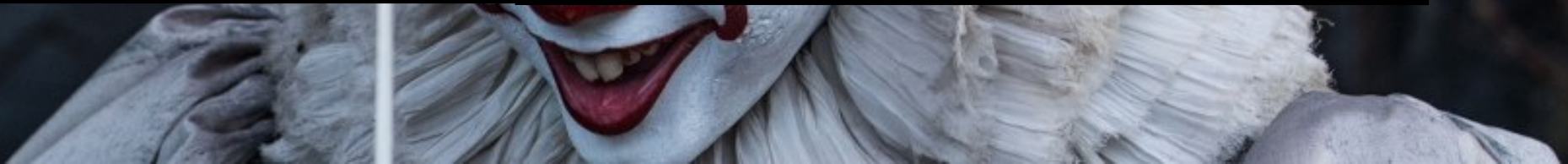
Normal Evil

Ab

evil



Abnormal Benign



# Evil..or not Evil?

Normal Benign

Normal Evil

Abnormal Evil

Abn

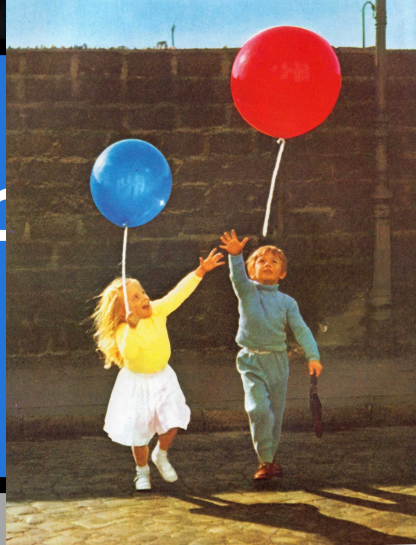
ign





# Evil..or not Evil?

Normal



Benign

Normal Evil

Abnormal Evil

Abnormal Benign



**Evil**..or not Evil?

Normal Benign

**Normal Evil**

\_(ツ)\_

**Abnormal Evil**

Abnormal Benign





An aerial photograph of a town. In the background, a large church with a tall steeple sits atop a green hill. The town below is filled with various buildings, including a prominent red brick building with a large mural that says 'DERRY'. A street runs through the center of the town, with cars visible. The sky is clear and blue.

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



An aerial photograph of a town. In the background, a large church with a tall steeple sits atop a green hill. The town below is filled with various buildings, including a prominent red brick building with a large mural that says 'DERRY'. A street runs through the center of the town, with cars visible. The sky is clear and blue.

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