09-07-18

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

**Rick McElroy,** Security Strategist
**@infosecrick**

Carbon Black.

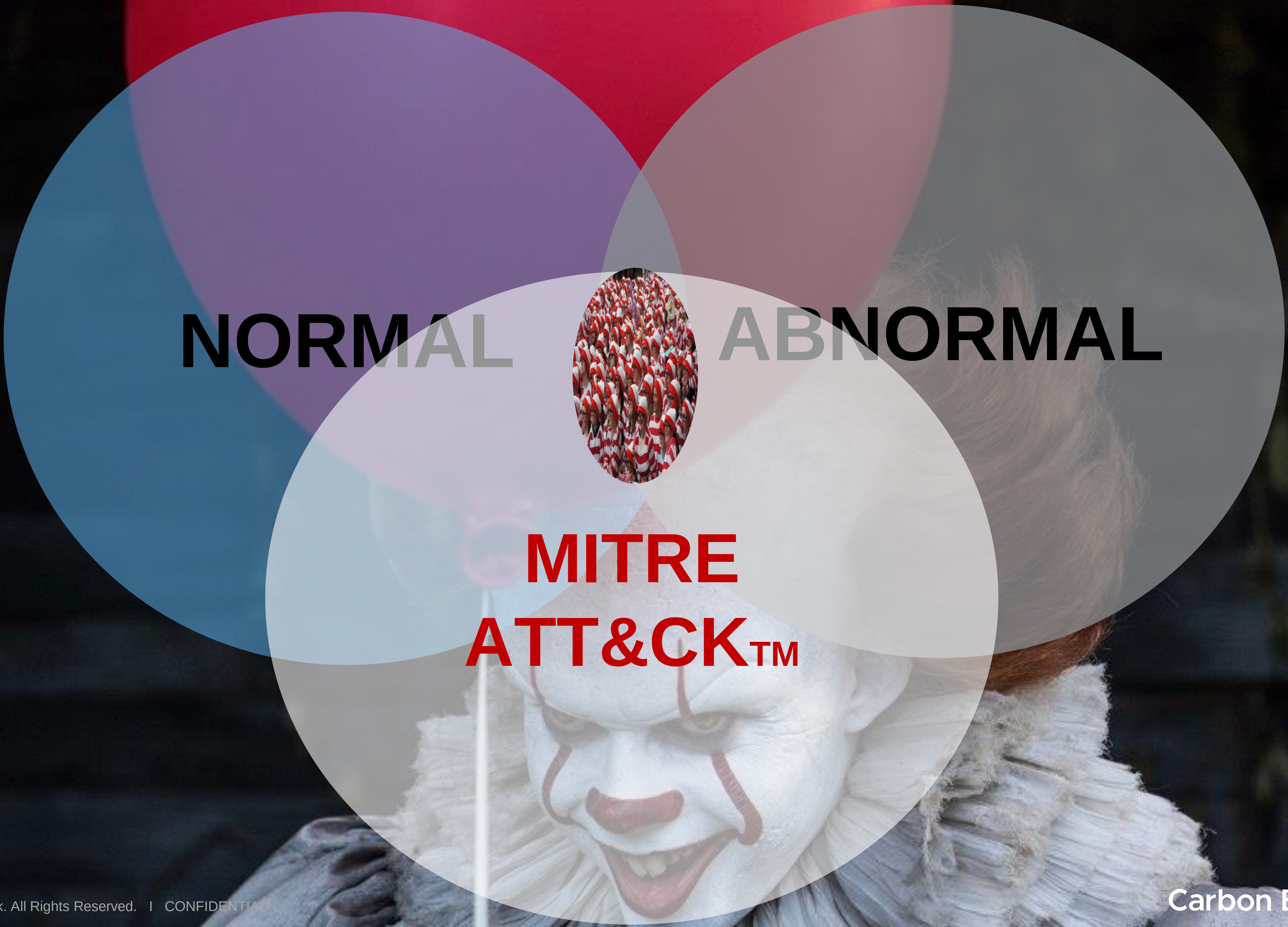
# Know normal.
# Find evil.

Carbon Black.

Carbon Black.

VISION

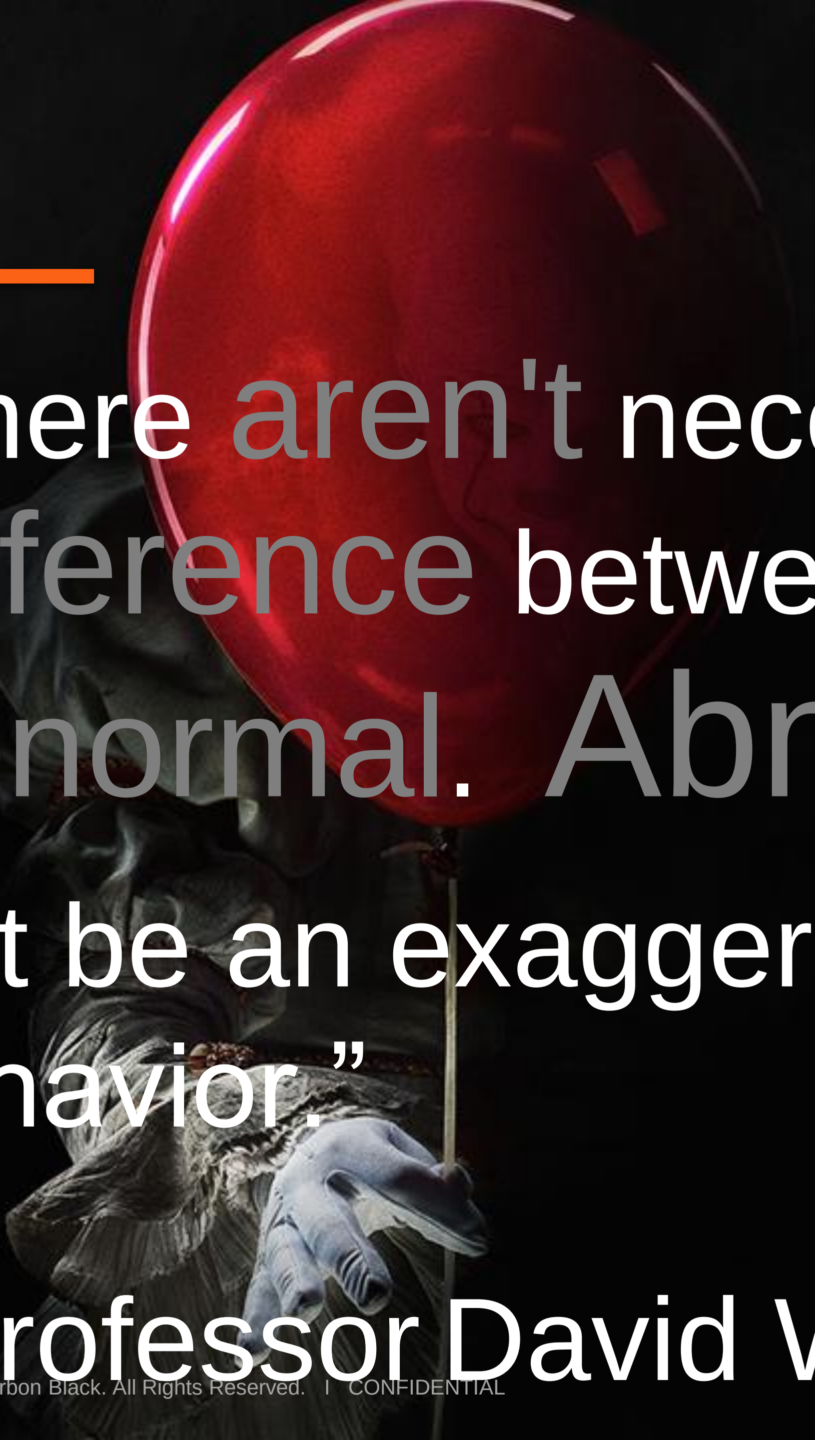
# A World Safe from Cyber Attacks



NORMAL

ABNORMAL

MITRE
ATT&CKTM



"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 Abnormal

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

# Evil

## Current Table

## Actual Table

| | |
|---|---|
| **Normal Benign**<br>(Lawful Good) | **Normal Evil**<br>**Frequent GOOD!!**<br>(Chaotic Good) |
| **Abnormal Evil**<br>(Chaotic Evil) | **Abnormal Benign**<br>**Infrequent BAD!!**<br>(Lawful Evil) |

IT
BKF

# Evil..or not Evil?

| | |
|---|---|
| Normal Benign | Normal Evil |
| Abnormal Evil | Abnormal Benign |

# Evil..or not Evil?

| | |
|---|---|
| Normal Benign | Normal Evil |
| Abnormal Evil | Abnormal Benign |

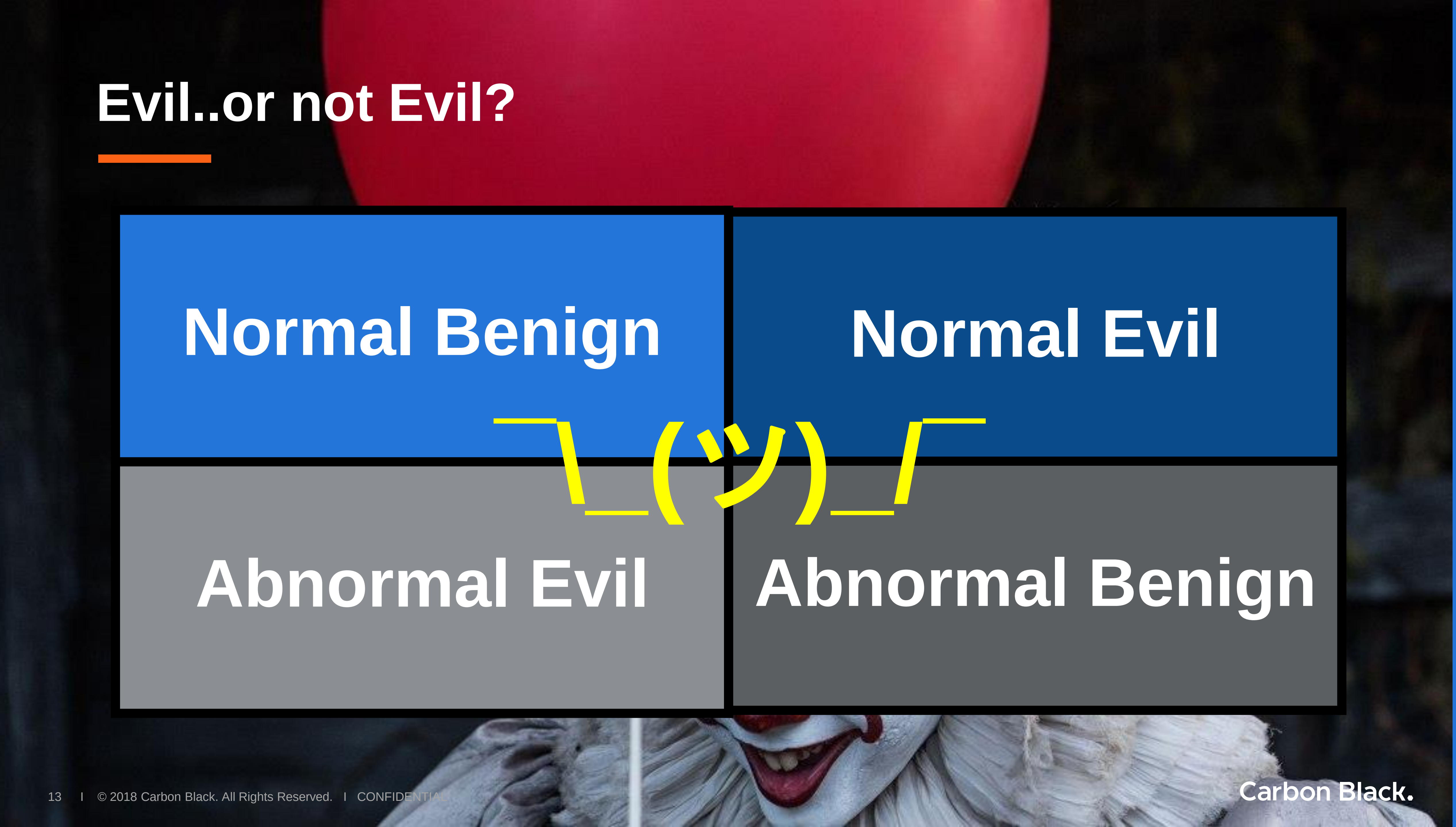
# Evil..or not Evil?

| | |
|---|---|
| Normal Benign | Normal Evil |
| Abnormal Evil | Abnor enign |

# Evil..or not Evil?

| | |
|---|---|
| Normal Benign | Normal Evil |
| Abnormal Evil | Abnor enign |

# Evil..or not Evil?



| | |
|---|---|
| Normal Benign | Normal Evil |
| Abnormal Evil | Abnormal Benign |

¯_(ツ)_/¯

# Know normal.
# Find evil.

Carbon Black.

UNNECESSARY
NOISE
PROHIBITED
POLICE DEPT

# Goals of Effort

We want everyone to contribute data back to MITRE

We want to help teach developers to do the right thing

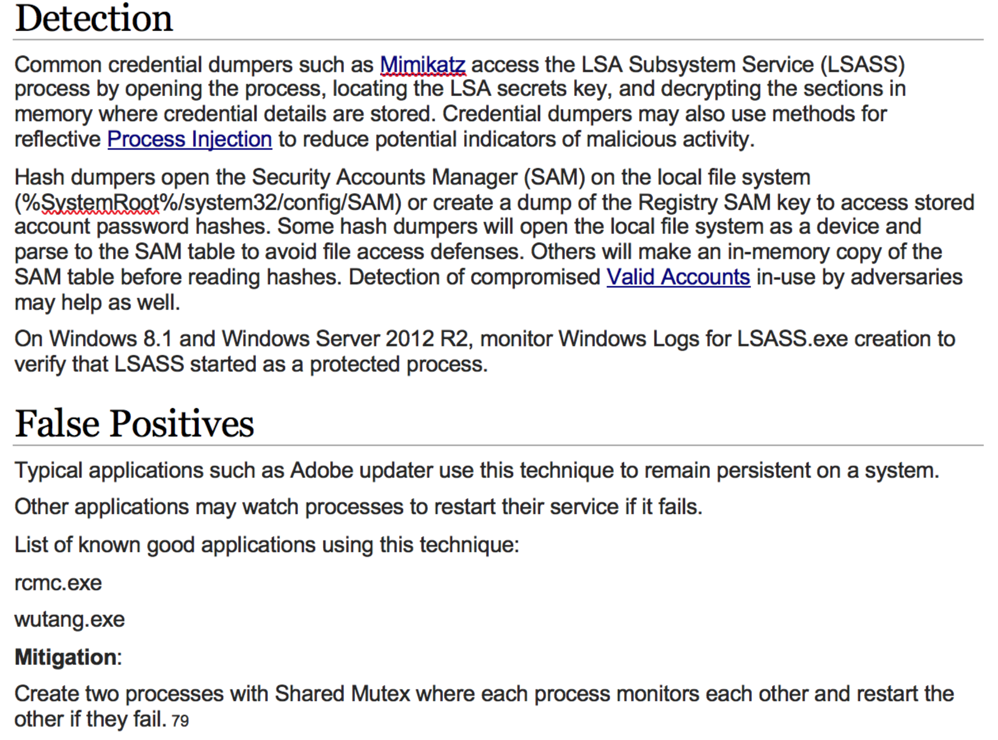
We want to reduce false positives for everyone

We want to save everyone time

# Our Commitment Slide

Host NORMINT Slack

Provide good known binaries back to MITRE



## Detection

Common credential dumpers such as Mimikatz access the LSA Subsystem Service (LSASS) process by opening the process, locating the LSA secrets key, and decrypting the sections in memory where credential details are stored. Credential dumpers may also use methods for reflective Process Injection to reduce potential indicators of malicious activity.

Hash dumpers open the Security Accounts Manager (SAM) on the local file system (%SystemRoot%/system32/config/SAM) or create a dump of the Registry SAM key to access stored account password hashes. Some hash dumpers will open the local file system as a device and parse to the SAM table to avoid file access defenses. Others will make an in-memory copy of the SAM table before reading hashes. Detection of compromised Valid Accounts in-use by adversaries may help as well.

On Windows 8.1 and Windows Server 2012 R2, monitor Windows Logs for LSASS.exe creation to verify that LSASS started as a protected process.

## False Positives

Typical applications such as Adobe updater use this technique to remain persistent on a system.

Other applications may watch processes to restart their service if it fails.

List of known good applications using this technique:

rcmc.exe

wutang.exe

**Mitigation**:

Create two processes with Shared Mutex where each process monitors each other and restart the other if they fail. 79

Carbon Black.

UNNECESSARY
NOISE
PROHIBITED
POLICE DEPT

SOUNDS GREAT
TONY
BUT... BUT... BUT...

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

— **Randy Pausch**

# Know normal.
# Find evil.

Carbon Black.

www.CarbonBlack.com

# Thank you.

rmcelroy@carbonblack.com
@infosecrick

Carbon Black.

# Questions?

Carbon Black.

www.CarbonBlack.com