Good vs Evil

Winning the Age-Old Battle

Doug Burks @dougburks
The Terms Good and Evil

- real yet abstract
The Terms Good and Evil

- real yet abstract
- carry weight
The Terms Good and Evil

- real yet abstract
- carry weight
- evoke emotion
The Terms Good and Evil

• real yet abstract
• carry weight
• evoke emotion
• convey true importance
Good vs Evil

https://www.theguardian.com/technology/2017/may/22/ransomware-attack-hero-marcus-hutchins-super-invasive-tabloids#img-1

https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#/media/File:Wana_Decrypt0r_screenshot.png

Doug Burks @dougburks
Good

• Security researchers like MalwareTech
Good

- Security researchers like MalwareTech
- SOC analysts, incident responders, management

Doug Burks @dougburks
Good

• Security researchers like MalwareTech

• SOC analysts, incident responders, management

• Emergency Responders
Good

- Security researchers like MalwareTech
- SOC analysts, incident responders, management
- Emergency Responders
- War heroes
Good

- Security researchers like MalwareTech
- SOC analysts, incident responders, management
- Emergency Responders
- War heroes
- Knight in Shining Armor

Doug Burks @dougburks
"You have not picked a career. You have picked a crusade."

-- Dan Geer, Source Boston Closing Keynote
Noble

• What we do is more important than:
  – paycheck
  – 401k
  – the rising cost of health insurance
  – promotion

Doug Burks @dougburks
Chivalry

We're not defending damsels in distress, but rather organizations in distress.
Chivalry

"Thou shalt respect all weaknesses, and shalt constitute thyself the defender of them."

--Leon Gautier's Ten Commandments of Chivalry

Doug Burks @dougburks
Chivalry

"Thou shalt not recoil before thine enemy."

--Leon Gautier's Ten Commandments of Chivalry
Chivalry

"Thou shalt be everywhere and always the champion of the Right and the Good against Injustice and Evil."

--Leon Gautier's Ten Commandments of Chivalry

Doug Burks @dougburks
Hero

• Chivalry is hard

• If it were easy, everybody would do it

• We need to celebrate our victories AND our heroes
Call it what it is

• Which computers did he slither into?
• How did the scoundrel become superuser?
• How did the SOB get Cray passwords?
• Did the skunk guard against detection?
• Can you audit a varmint who's sys manager?

Screenshot from https://www.youtube.com/watch?v=1h7rLHNXio8
Doug Burks @dougburks

http://www.newsweek.com/history-computer-hacking-69449
Be heroic, but remember...

...heroics are not sustainable

https://twitter.com/taosecurity
Doug Burks @dougburks
By analysts, for analysts

https://taosecurity.blogspot.com/2017/02/guest-post-bamm-visscher-on-detection.html

Doug Burks @dougburks
Expect the Unexpected

https://twitter.com/markbaggett

Doug Burks @dougburks
Legacy

• Long-term is not just the next project you work on
Legacy

• Long-term is not just the next project you work on

• It's not the next promotion or next employer
Legacy

• Long-term is not just the next project you work on
• It's not the next promotion or next employer
• It's the stories that future generations will tell about those Internet heroes back in 2017

Doug Burks @dougburks
How do we build a legacy of fighting evil?

We must...
Look
Question
Accelerate
Persist

Doug Burks @dougburks

https://upload.wikimedia.org/wikipedia/commons/e/e2/Yosemite_El_Capitan.jpg
Looking at the Big Data Buffet

- IDS alerts
- DNS, HTTP, SSL
- FPC
- firewall logs
- proxy logs
- host telemetry
Questioning

- Does this make sense?
- Is this expected on this machine/network?
- Switch up your tactics every now and then
- Try a different hunting method
Accelerate
• Share information
• Open Source is a force multiplier
Time

• What percentage of your day is spent on meetings, administrivia, and water cooler talk?

• What percentage of your day are you finding evil?

• What percentage of that time is passively reacting to IDS alerts vs proactively hunting?

Doug Burks @dougburks
Break the Ludic Loop

• Don't mistake the urgent for the important (see Stephen Covey)

• Go for a walk

Doug Burks @dougburks
Learn Something New Every Day

• Your brain is a muscle
• It must be exercised
• Scripting, protocols, forensics, reverse engineering
Dynamic Range

- Be an A player
- Attract and retain A players

Doug Burks @dougburks

Automate

• Find that task that you do 10-100 times per day and automate it

• Time savings add up quickly

• Leaves you with more mental energy to do more advanced tasks
Persist

"When you're smart, people need you."

--- Real Genius
Change

• One of the things that makes us want to give up is change

• Don't try to boil the ocean

• Start small and iterate quickly
Communication

• Reading, writing, and speaking

• Lateral

• Vertical

• Outside your organization
Standing on the shoulders of giants

• Without those that have come before, we wouldn't be where we are today
Standing on the shoulders of giants

• Without those that have come before, we wouldn't be where we are today

• But that also means that we have the responsibility to be the shoulders for those who come after us
In the end, it all comes down to YOU

Doug Burks @dougburks
Are you going to sit idly by while evil is breaking into your network?
NO!
Are you going to let them walk out the door with your data?

Doug Burks @dougburks
NO!
Are you going to do nothing while other organizations are being compromised?

Doug Burks @dougburks
NO!
Are you ready to start your heroic journey?

Doug Burks @dougburks

https://upload.wikimedia.org/wikipedia/commons/5/53/Fog_on_Spencer_Butte%2C_Oregon.JPG