How to Literally Think Like an Attacker to Become a Better Defender
Eric Groce
INCIDENT HANDLER
RED CANARY
@infosechustle

- I am regularly involved with hundreds of IRs
- Former Fortune 500 endpoint security lead
- I was *that* end user
“The attacker only has to find one way to get in, while the defender has to defend everything.”

—Too many security people
Defenders and attackers are not all that different

- Similar technology
- Both are goal based
- Both have budgets
- Organizational structure
- Similar levels of skill
- At the end of the day, both perform a job
Counterfactual Thinking

A concept that involves the human tendency to create possible alternatives to life events that have already occurred; something that is contrary to what actually happened.
COUNTERFACTUAL PATHWAYS

Counterfactual

Content-Specific
- Intentions
- Causal inferences

Content-Neutral
- Mindsets
- Motives
- Contrast effects
- Perceived control

Behavior
**Counterfactual Types**

**Upward vs. Downward**
Comparison of a present outcome to a better or worse alternative

**Inaction vs. Action**
Addition or a subtraction of an aspect of the present state

**Self vs. Others**
Focus is on the action of oneself or others
Upward vs. Downward

**Defender thinks**
*(downward)*

“If this wasn't a holiday weekend, a lot more end users would have opened this phishing email.”

**Attacker thinks**
*(upward)*

“I would’ve had domain admin by noon if I had just used my other macro.”

**You might try thinking**

“Even more emails would have been stopped if I added that other email block policy before the weekend.”
Inaction vs. Action

Defender thinks

(*inaction*)

“I should not have ignored this malware report yesterday. If I didn't, I would know more about this malware.”

Attacker thinks

(*action*)

“I should have learned python instead of focusing on learning perl.”

You might try thinking

“I should have read this report yesterday instead of tuning the firewall.”
Self vs. Others

Defender thinks (Others)
“If it weren't for this end user clicking on this phishing email, I wouldn't be up at 2 AM!”

Attacker thinks (Self)
“If I can just improve my obfuscation within this weaponized word doc, it won't get stopped this time.”

You might try thinking
“If I had just trained our end users on better ways to spot phishing attacks, this wouldn't have happened”
The Forward Thinking Mindset

- Ownership
- Pride
- Confidence
Ownership
Accountability for one’s own actions

Pride
Satisfaction from the achievements in your job role

Confidence
Believe that you are doing good work
“The attacker only has to find one way to get in, while the defender has to defend everything.”
“The attacker only has to find one way to get in, while the defender has to defend everything.”

“But the attacker must get everything right, while the defender only has to detect one part of the attack.”