Security Response Survival Skills:
Zen and the Art of Incident Response

Microsoft Security Response Center
Ben Ridgway
Lizard Brain – Fight flight or freeze

Monkey Brain – Dishonor is death

Human Brain – Leisurely logical
SIR is a human problem

And when we get it wrong...

• Poor decision making skills
• Failure to follow process
• Costly operational mistakes
• Failed court cases
• Burnout
Strategies for successfully navigating the human factor
Learn to spot Monkey Brain

- Physical response
- Like/Dislike teammates
- Must prove you are right
- How trumps what
- Labeling of others
- Excuses/Justifications
Step 1
De-escalate yourself
Reasoning with the Monkey Brain

- Use Team Speak
- Highlight triumphs
- Don’t postmortem until the post mortem
- Empathize with detractors
- Be open with your plans

Throw the monkey a banana
Filling leadership vacuums

• Monkeys and lizards thrive in leaderless situations

• Will the loudest monkey please stand up?

• Step in:
  • It doesn’t matter where, just move
  • Remember: everybody is faking it
  • BUT: don’t lead through ignorance
  • When all else fails: ask questions
Discipline isn’t accidental

IR teams try to move fast and loose

Make documentation a core function
  “Discovery” cases: 1 per 4-6 analysts
  Everything else: 1 per 6-8 analysts

Proper prior preparation
Combatting Fatigue
Fatigue is your most dangerous adversary

- Day 1: no more than 16-hours straight
- Day 2-7: no more than 10-hours straight
- Day 7-n: no more that 10-hours straight for 4 consecutive days
The simplest and most effective way to combat IR team fatigue:

**Regularly reevaluate the objective**

- Is what we are doing getting us there?
- Is there anything we are doing that we don’t need to do?
Long term impact of stress and fatigue

- Memory and concentration impairment
- Anxiety
- Depression
- Digestive problems
- Headaches
- Heart disease
- Sleep problems
- Weight gain
Avoiding The Security Team Death Slide
Sources and Further Reading


• “Chronic stress puts your health at risk.” Mayo Clinic. April 21, 2016.


• Walker, Matthew PhD, Why we Sleep, the Power of Sleep and Dreams. Scribner. 2018.
The human problem

“A bug is never just a mistake. It represents something bigger. An error of thinking that makes you who you are.” – Elliot Alderson, Mr. Robot
Thank you