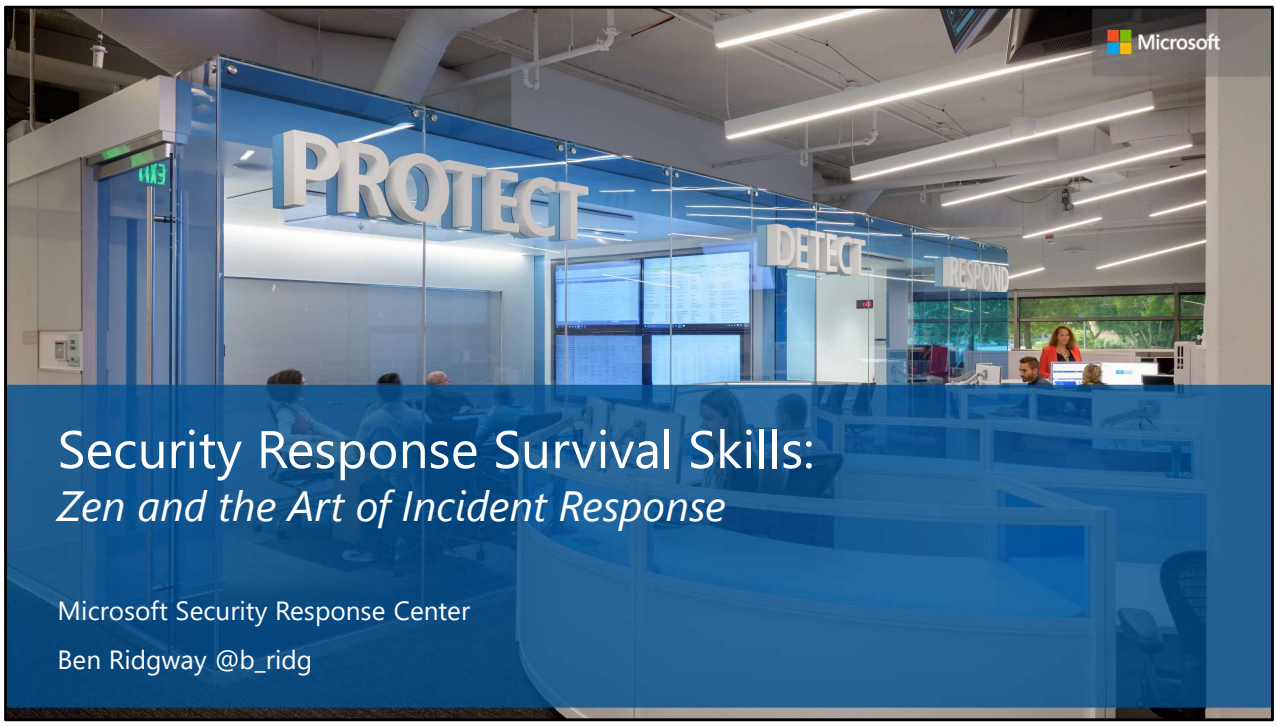


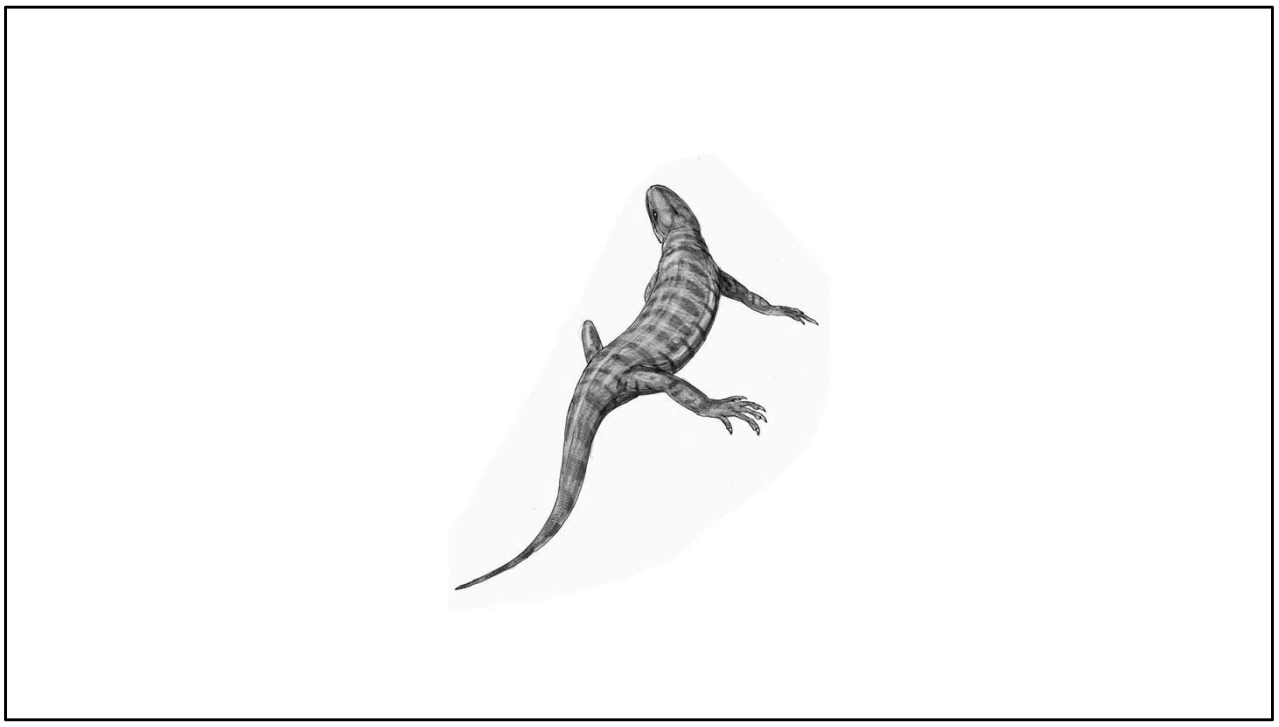
Security Response Survival Skills:
Zen and the Art of Incident Response

Microsoft Security Response Center

Ben Ridgway @b_ridg

- Security conferences are filled with people talking about technical solutions to security problems
- Box that will find all my bad guys
- Box that will fuzz my software and find all the bugs
- Nobody sells a box that will help a vice president make a logical informed decision when
    - He/she is facing the possibility of a data breach
    - The loss of his or her business
    - The loss of his or her job
    - The loss of the jobs of all of his or her reports
    - If you do sell this appliance, please come talk to me.

- Not every incident involves technology
    - Every incident involves the rational and logical collaboration of humans

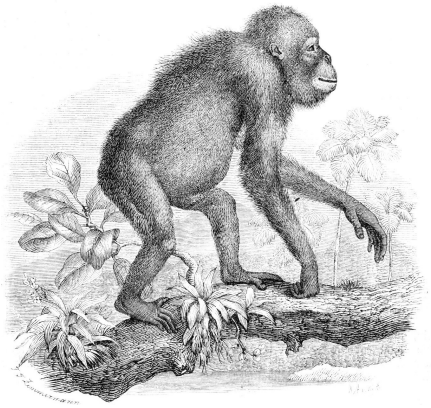


https://en.wikipedia.org/wiki/Casineria

To begin, I'd like everyone to use their imagination.

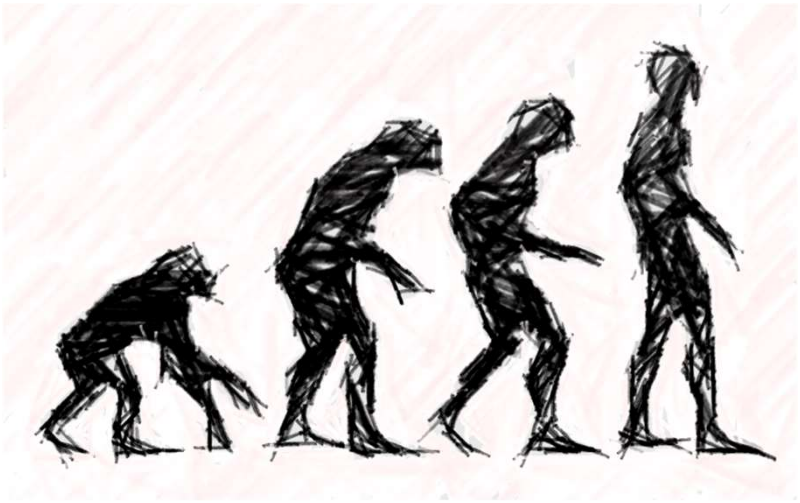
It is 340 million years ago. You are this little guy. A casineria.
One of the last common ancestors between mammals and reptiles
You're sitting in a tree looking for tasty bugs and feel eyes on you.
Luckily, your brain has evolved a center to make split second fight, flight or freeze decisions.
Psychologists call this the lizard brain, but it likely developed much earlier
More technically, the hindbrain or Amygdala

Image Credits:
https://en.wikipedia.org/wiki/Casineria



Fast forward 300 million years
You are now an early primate
Through some complicated set of hand gestures and vocalizations a member of your family group is accusing you of stealing the last tasty piece of fruit
You are very upset because you didn't steal the fruit
You also know that your family unit has no tolerance for that sort of thing and will kick you out to fend for yourself
Your amygdala is also active but working in a different way
Psychologists this monkey brain
It was certainly present in our tribe-dwelling ancestors, but a form is probably present in many other places too.
You fight back like your life depends on it, because it does

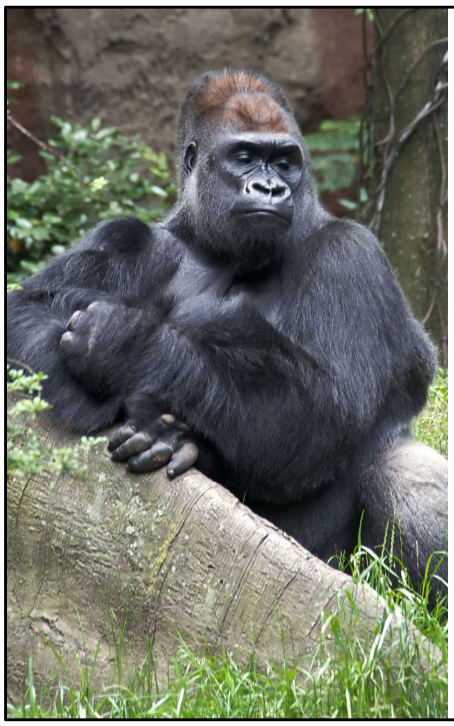
Image Credit
https://upload.wikimedia.org/wikipedia/commons/9/98/Orangutan-drawing.jpg



- Fast forward to today.
- Humans now have massively developed hippocampus
- That hippocampus is responsible for what we call logical or rational thought
- Largest part of the brain
- Uses the most energy
- The reason you need to sleep on it
- Has the most connections
- Is also the slowest, and unequipped for dealing with split second decisions.
- It has invented the digital watch and the internet

- The lizard brain and monkey brain haven't gone away.
- They are just hidden, most of the time
- They still come out when you perceive danger

Image Credit:
https://commons.wikimedia.org/wiki/File:Human_evolution.svg



Lizard Brain – Fight flight or freeze

Monkey Brain – Dishonor is death

Human Brain – Leisurely logical

- To recap
- Humans still maintain their lizard and monkey brains
- These functions still activate in moments of stress, fatigue or perceived danger

- The Human brain is logical but very slow
- It is the reason you need to “sleep on it”

- Lizard
    - Fight flight or freeze
    - Handy if you’re an athlete or in physical danger
    - Also very handy if you are an athlete
    - Luckily, this rarely applies to IT security incidents
- Monkey brain
    - Doesn’t know the difference between death and dishonor

- Security people consistently get it wrong
    - We charge in and cast blame on those responsible
    - How many have been to defcon and seen the walk of shame talks?

    - We act like we're the heroes swooping in to conquer
    - How many of you love to be responders because you get to exercise your hero complex?

- This isn't a technical problem. Change. This is a human problem

Image Credit:
https://upload.wikimedia.org/wikipedia/commons/c/c0/Western_Lowland_Gorilla_at_Bronx_Zoo_2_cropped.jpg

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

- Nobody comes to security response because they are having a good day
  - Security incidents are emotionally charged
  - Scary, violating, unusual
  - Often caused by somebody making a mistake

- Let's talk about better way to manage incidents
  - So that we avoid common pitfalls
  - Respond quickly and efficiently
  - Build a case that will hold up in court
  - Maintain a healthy and happy team

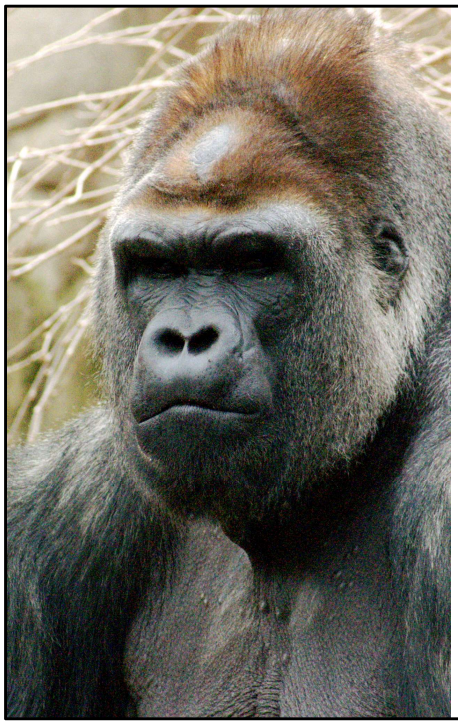
Image credit:
https://commons.wikimedia.org/wiki/File:US_Navy_091028-N-9860Y-005_Navy_Region_Northwest_Fire_and_Emergency_Services_and_Oak_Harbor_Fire_Department_personnel_decontaminate_the_Navy_Region_Northwest_Fire_and_Emerge

ncy_Services_initial_entry_team.jpg

Here is how understanding the brain and the way humans respond to stressful situations can make you a more effective responder

How can you identify monkey brain in yourself and others
What do you do about it

Image note:
Petty Officer 2nd Class Shauntae Hinkle-Lymas, U.S. Navy (https://commons.wikimedia.org/wiki/File:Defense.gov_News_Photo_110406-N-YS896-131_-_First_Phase_Basic_Underwater_Demolition_SEALs_BUD_S_candidates_use_teamwork_to_perform_physical_training_exercises_with_a_600_pound_log_at_Naval.jpg), „First Phase Basic Underwater Demolition/SEALs (BUD/S) candidates use teamwork to perform physical training exercises with a 600 pound log at Naval Amphibious Base Coronado on April 6, 2011 “, https://www.usa.gov/government-works. Public Domain



Learn to spot Monkey Brain

- Physical response
- Like/Dislike teammates
- Must prove you are right
- How trumps what
- Labeling of others
- Excuses/Justifications

“If you care, if you feel emotion, if you are passionate about your causes, the part of the brain that makes good decisions is offline” – Conflict Communication pg 39
You want people to care, but you don’t want them acting purely off of emotions.

The Monkey brain is a self protection mechanism that is very handy if you’re trying to keep from getting kicked out of the tribe for stealing a banana,
but not so handy if you’re responding to a security incident.

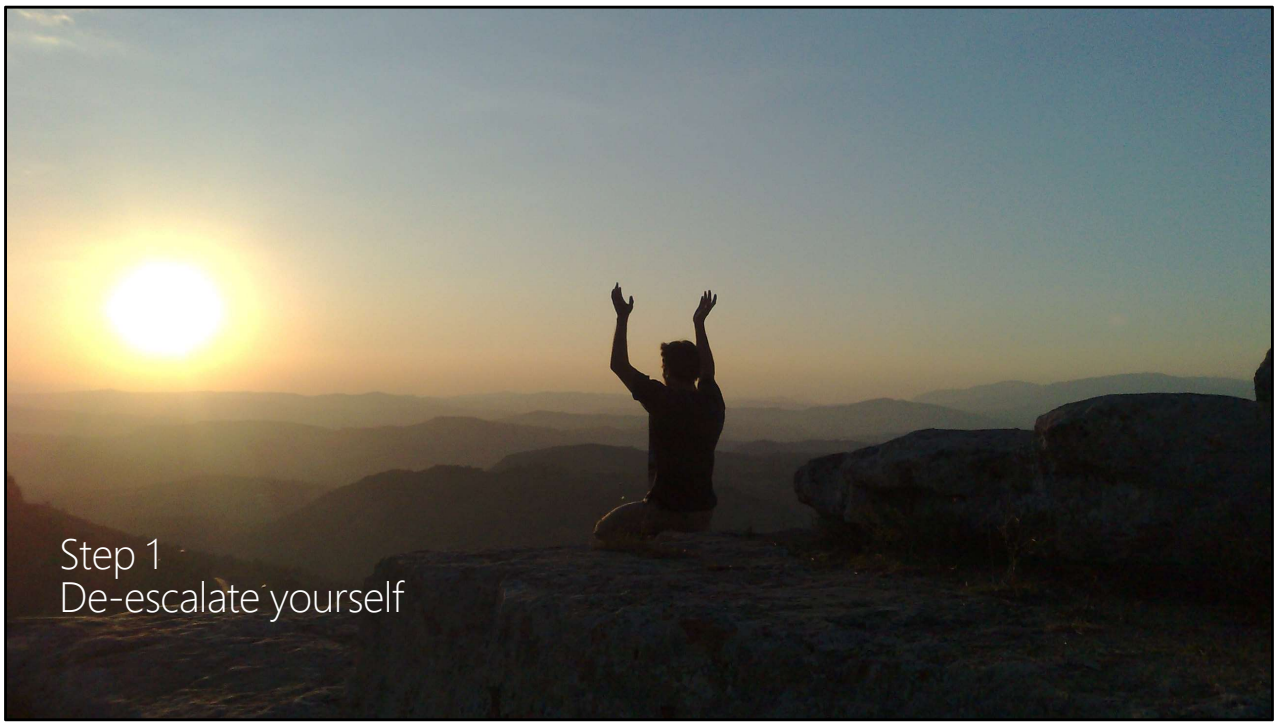
The Monkey will fight so ruthlessly to preserve self or honor, that it renders the part of the brain responsible for logical decisions inert.
As I was preparing this talk,

Let’s talk about how we identify monkey brain in ourselves and other people.

Physical – body language. Flushed.
Like/Dislike – it doesn’t matter if it is positive or negative. It is a matter of social dynamic

Focus shifts to proving you are right – “if you want the problem solved and don’t care who gets credit for it, you are thoroughly in the human brain” cc pg 39
How trumps what – The monkey cares whether it is over the top/under bottom. Human just wants there to be TP
Labeling – Racial, sexist, or related to position/hierarchy. “Oh, he’s just a PM”
Excuses/Justifications – hard to do in the moment if self

Image Credit:
https://upload.wikimedia.org/wikipedia/commons/4/41/Gorilla_019.jpg



- People have an unconscious ability to respond when someone else is triggered
    - No way to de escalate somebody else if you are triggered

- Monkey is insidious and insists that it isn't in control
    - Being triggered into monkey is dishonorable
    - Exactly the sort of thing Monkey doesn't want to admit

- You are in monkey brain because it is trying to protect you.

- Recognize the problem
- Take 5
- Admit that you're triggered
    - If monkey is dishonorable, admitting it and being accepted disproves monkey
    - This is why admitting it is so powerful.
    - It proves to monkey that it isn't death

Been in this situation a few times?
- Maybe it is time to step aside

Image Credit:
https://commons.wikimedia.org/wiki/File:Pagan_meditation.jpg

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

https://www.shutterstock.com/image-photo/gorilla-using-branch-tool-127553582?src=i22hwzLu6frbhj4WZmuWwA-1-2

- How do you deal with monkey brain in others?
- As I mentioned, we do this exactly backwards
    - Engage in shaming those responsible
    - Want to route out the causes
    - Come in with a sense of security elitism
    - "Don't worry, I'm here to save the day"

- Better method
    - Deliberate team speak
    - Highlight triumphs
    - Be generous with compliments
    - Don't postmortem in the incident
    - Take time to understand detractors

    - In short, I like to think about throwing the monkey a banana.
    - Give the monkey something that will make it happy and appease its

concerns.

Image credit:
https://upload.wikimedia.org/wikipedia/commons/6/64/Cebus_albifrons_edit.jpg

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

- This applies mostly to incident managers or leads
- Human brains thrive with strong perceived leadership
  - At an emotional level: don't worry because somebody knows what they're doing (even if they don't)
  - Worst possible case: nothing is happening
  - Second worst possible case: everybody is doing their own thing without direction
- Lack of leadership
  - Loudest voice usually prevails
  - Louder != right
- What if you don't know what to do?
  - Nobody knows. Everybody is faking it
  - Pick a direction and go
  - BUT
  - Listen and pay attention
  - Less leading through arrogance

- Tell Chaos Story

Image note:
U.S. Navy photo by Mass Communication Specialist 1st Class Michael Russell, (https://www.flickr.com/photos/usnavy/12106700734/), https://www.usa.gov/government-works. Public Domain

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

"7Ps"

Proper prior preparation prevents poor performance

Ben

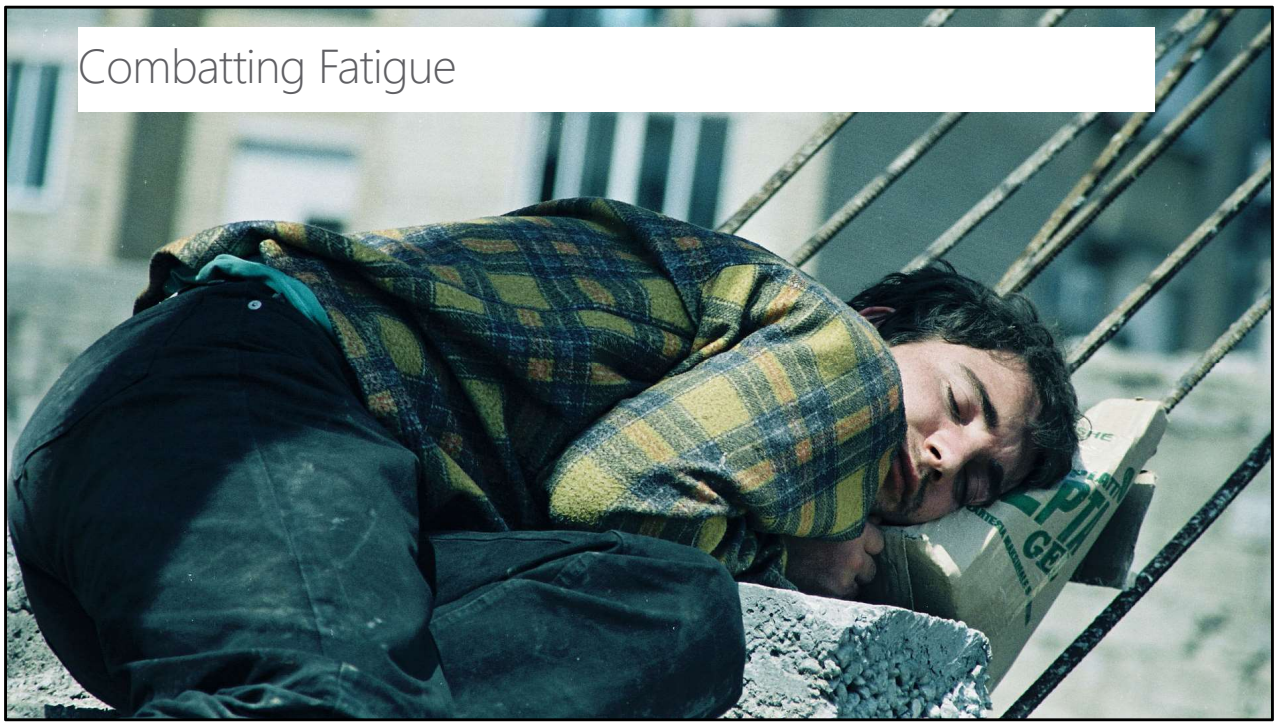
Acknowledge that they may already know this. Important point is that this isn't natural

- Even incidents where nobody is upset can go off the rails
- When confronted with danger natural reaction
    - Get out of danger as fast as possible
    - Avoid any distraction between you and victory
- Problems
    - Meticulous documentation isn't natural for most analysts
    - People get more fatigued when they are doing something that isn't natural
    - Causes trouble when you expect going to court
    - Legal cases require
        - Chain of custody
        - Meticulous notes
        - No undocumented logical leaps
        - All of this is problematic for analysts
    - Solution
        - make documentation a core function and assign dedicated resources

        - Practice IR like you want to run it
    - Documentation
        - Keep minutes
        - Track IOCs
        - Keep track of the forensic queue and assign
        - Ensure consistency
        - Cases which may go to court
            - 1 per every 4-6 analysts
        - Everything else
            - 1 per 6-8
    - Practice
        - Practice like the real thing
        - Make muscle memory work in your favor
- Incidents decent into chaos thanks to lack of leadership.

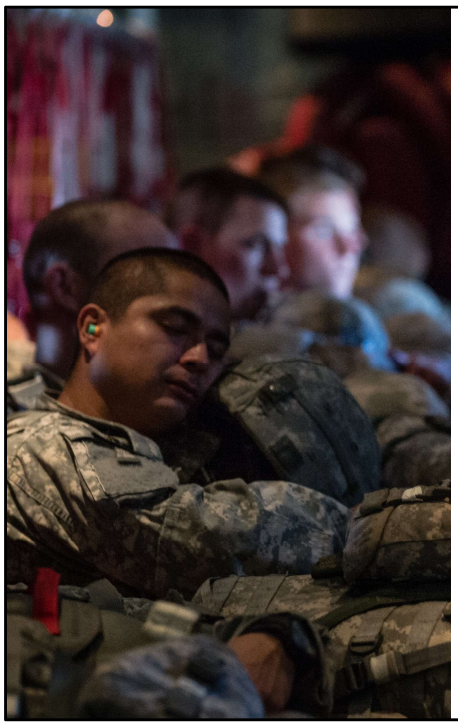
Image Credit
https://upload.wikimedia.org/wikipedia/commons/8/83/Day_253_-_West_Midlands_Police_-_Forensic_Science_Lab_%287969822920%29.jpg

Combatting Fatigue



- A very interesting thing happens when we are fatigued.
- Comes from the fact that the hippocampus (or human brain) requires a lot of energy
- And is one of the main customers for sleep and down time
- Function of the human brain decreases
- Function of hindbrain increases
- People get a lot more likely to become triggered
- Ability to make rational decisions decrease
- Thus, no conversation about human factors could be complete without discussing fatigue.

Image credit:
https://en.wikipedia.org/wiki/Power_nap#/media/File:Sleep_in_ruins.jpg



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

- Natural inclination for most teams is to burn hard
- Groups without “follow the sun” models will try to work 24x7 to resolve security issues
- Adrenaline and thrill of the chase mask warning signs of fatigue
- Everyone will eventually succumb to tiredness
- Would you really want your entire incident response team to be drunk?

- SIR is a precision sport
- Details are easy to overlook
- Evidence and chain of custody easy to screw up
- Code fixes are easily inject new bugs

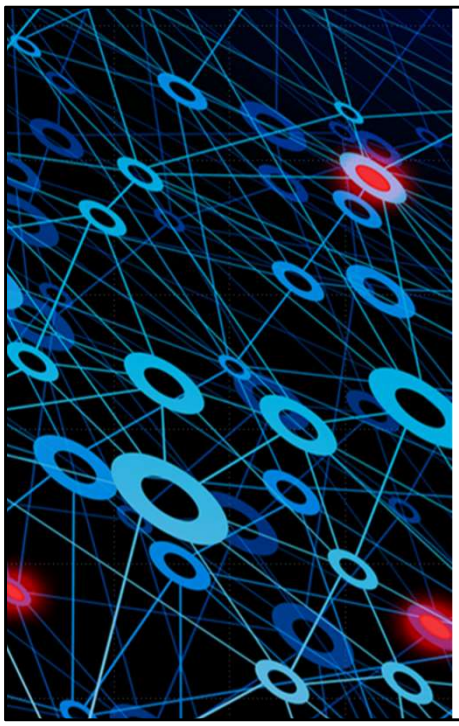
- Break this down logically
- Your team is guaranteed to screw something up if they are fatigued
- An adversary is never guaranteed to be successful
- Thus, more important to take care of your team than burn hard recklessly

- A good Security Incident Manager will anticipate team member fatigue before the team member does themselves
- Set rules for yourself, find a manager to hand off to
- Manage your leadership
- I have deliberately set status updates far apart to force VPs to sleep

- Tell story of the overworked IR lead
- Legal having him declared a threat to the business

Blazejewski S, Girodet P, Orriols L, Capelli A, Moore N, CESIR Group FT. Factors Associated With Serious Traffic Crashes: A Prospective Study in Southwest France. *Arch Intern Med.* 2012;172(13):1039–1041. doi:10.1001/archinternmed.2012.1695 https://jamanetwork.com/journals/jamainternalmedicine/fullarticle/1162167

Image credit: https://commons.wikimedia.org/wiki/File:U.S._Army_paratroopers_with_the_1st_Battalion,_503rd_Infantry_Regiment,_173rd_Airborne_Brigade_Combat_Team_sleep_during_a_flight_over_Germany_aboard_an_Air_Force_C-130J_Super_Hercules_aircraft_assigned_to_140905-F-YC884-175.jpg



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?

Those rules of thumb aside. There is one simple and incredibly effective way to combat fatigue

***Click ***

Regularly reevaluate the objective

- Incidents establish their own momentum
- Hundreds or thousands of compromised systems
- Security people tendency to want to leave no stone unturned
- Most IR engagements waste a lot of effort
- Effort is costly in time and the most precious resource: energy
- Incident managers should constantly be evaluating what the objective is

click

- Is what we're doing getting us there?
- Is there anything we're doing that we shouldn't be doing?

Image Note:
Microsoft stock image

Long term impact of stress and fatigue

- Memory and concentration impairment
- Anxiety
- Depression
- Digestive problems
- Headaches
- Heart disease
- Sleep problems
- Weight gain

When humans experience emotional stress, their brains create the stress hormone cortisol
Your body doesn't care whether stress is real or perceived, physical or emotional.
It reacts the same way
Research is discovering the long term impact of cortisol
Decreased function of the hippocampus AKA the human brain
Memory and concentration impairment but others too

Let me say that another way
When we drive ourselves and our teams too hard for too long, we're killing the part of the brain we need most.

- Anxiety
- Depression
- Digestive Problems
- Headaches
- Heard disease
- Sleep problems
- Weight gain

All bad if you care about yourself, your team, or your insurance premiums

Image credit:
https://commons.wikimedia.org/wiki/File:Zoll_E-Series_(2).JPG

A few years ago I visited the SIR team of a large customer. Let's call them "Contoso" because I won't use their real name.
The goal was to discuss information sharing, and ways to better partner.
Initially I was troubled by how unequipped they seemed
Individually, everyone seemed incredibly capable
Over lunch with the team the conversation turned toward their histories
I made a shocking discovery everyone on the team had joined from another company "Fabrikam" within the last 6-months.
Contoso and Fabrikam were almost the same size.
Fabrikam had lost their entire SIR team to Contoso.
In order for this to have happened, Contoso had lost their entire SIR team to somebody else.
The IR team death slide

1. Team is overworked or unhappy
2. Somebody gets a great deal and moves somewhere else
3. Everyone else is even more overworked because it takes a long time to backfill security response positions
4. Repeat a few times
5. You lose a significant portion of your team. Everyone is significantly overworked

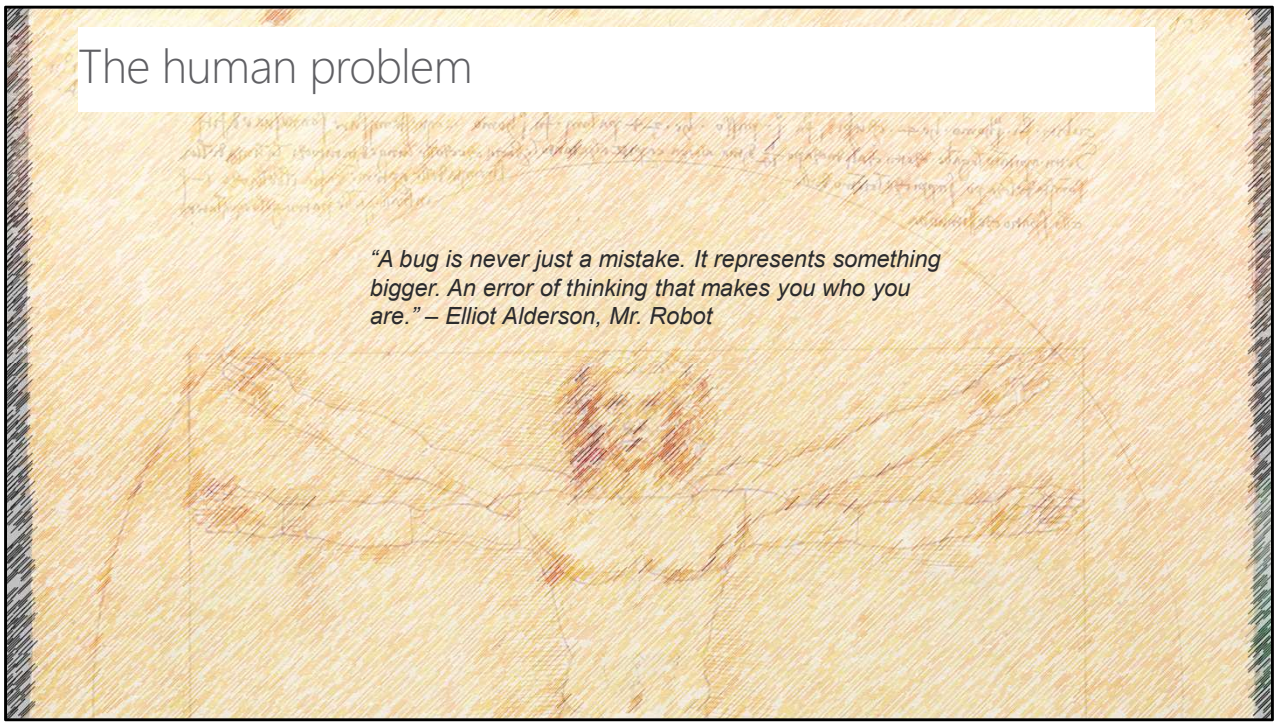
If this happens, you need to do something drastic.
You don’t want to be Contoso or Fabrikam

Within 6-months of my visit
Both Contoso and Fabrikam suffered data breaches

Image credit:
https://upload.wikimedia.org/wikipedia/commons/3/34/Warning_-_Area_Closed_-_Dangerous_Cliffs.jpg

Sources and Further Reading

- Bergland, Christopher. "Cortisol: Why the "Stress Hormone" Is Public Enemy No. 1." Psychology Today: The Athlete's Way. January 22, 2013. https://www.psychologytoday.com/intl/blog/the-athletes-way/201301/cortisol-why-the-stress-hormone-is-public-enemy-no-1
- Calveiro, Lissette. "Studies Show Sleep Deprivation Performance Is Similar to Being Under the Influence of Alcohol." Huffington Post. March 31, 2016. https://www.huffingtonpost.com/lissette-calveiro/studies-show-sleep-deprivation-performance-is-similar-to-being-under-the-influence-of-alcohol_b_9562992.html
- "Chronic stress puts your health at risk." Mayo Clinic. April 21, 2016. https://www.mayoclinic.org/healthy-lifestyle/stress-management/in-depth/stress/art-20046037
- Miller, Rory. Conflict Communication (ConCom): A New Paradigm in Conscious Communication. Ymaa Publication Center. June 15, 2015.
- Walker, Matthew PhD, Why we Sleep, the Power of Sleep and Dreams. Scribner. 2018.
- Wikimedia.org (for almost all my graphics)



I'd like to close with a security presentation cliché: A quote from the TV Show Mr. Robot.

"A bug is never just a mistake. It represents something bigger. An error of thinking that makes you who you are."

Security incidents and bugs are ultimately caused by humans
They are scary situations
Plenty of opportunities for perceived danger
When humans are in dangerous situations, less evolved parts of the brain can take over
This can have disastrous implications
As responders we can do better by recognizing this
Learning to engage with humans in the right way
Helps you respond quickly, effectively, and efficiently
While maintaining a healthy and happy team

Image Credit:
https://upload.wikimedia.org/wikipedia/commons/thumb/2/22/Da_Vinci_Vitruve_Luc

_Viatour.jpg/1200px-Da_Vinci_Vitruve_Luc_Viatour.jpg

Image Credit:
Microsoft Stock Photo