



Qasim “Q” Ijaz



# \$WHOAMI

- Lead penetration testing teams at Coalfire Labs
- “Adaptive penetration testing” instructor at BH U.S. and BH EU
- Hundreds of penetration tests
  - As well as tens of HIPAA and HITRUST assessments
- Twitter: @hashtaginfosec



C O A L F I R E  
LABS

# AGENDA



TEAMWORK



TIME  
MANAGEMENT



ETHICAL DECISION  
MAKING



LEADERSHIP



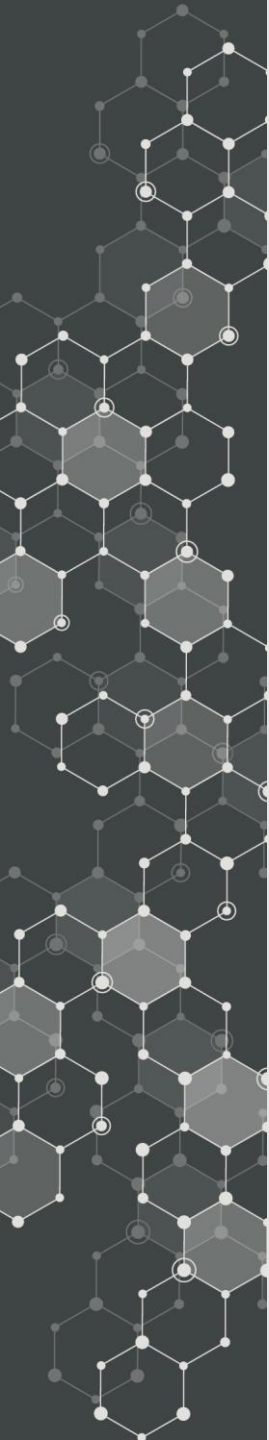
COMMUNICATION  
HACKS



QUESTIONS



CAL FIRE  
LABS

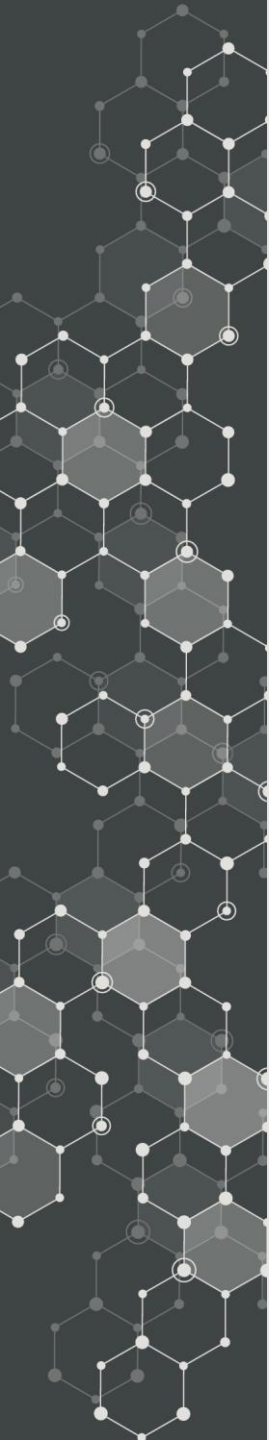


# TEAMS

- A collection of people who interact to achieve a common goal
  - E.g. a project manager, delivery director, and two penetration testers working on an app and network pen test
- Teams are part of everyone's life
- Different pieces of projects require
  - Complementary skills and competencies
  - Coordination of efforts
  - Establishing priorities
  - Combining knowledge and expertise







Fun2Fun.info

# TEAMWORK

It gets sh done.



CALFIRE  
LABS

# ENABLING CONDITIONS OF GREAT TEAMWORK

- Compelling Direction
  - That energizes, orients, and engages team members
  - Reduce confusion, set challenging goals
- Strong Structure
  - Diversity reduces “group think”
  - Optimally designed processes
  - Norms that discourage destructive behavior and encourage positive dynamics



C  A L F I R E  
LABS

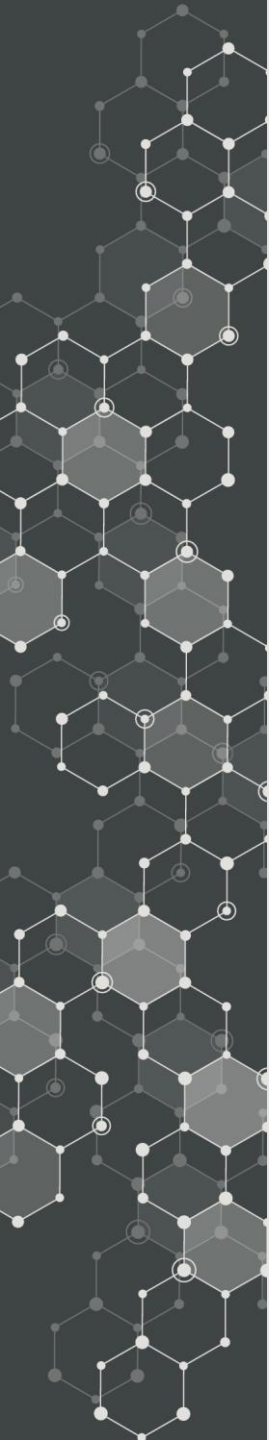
# ENABLING CONDITIONS OF GREAT TEAMWORK

- Supportive Context
  - A reward system that reinforces good performance (e.g. bonuses)
  - An information system that provides access to the data needed for work
  - Training (internal and external)
  - Technological assistance
- Shared Direction
  - Fostering common identity and common understanding



CAL FIRE  
LABS



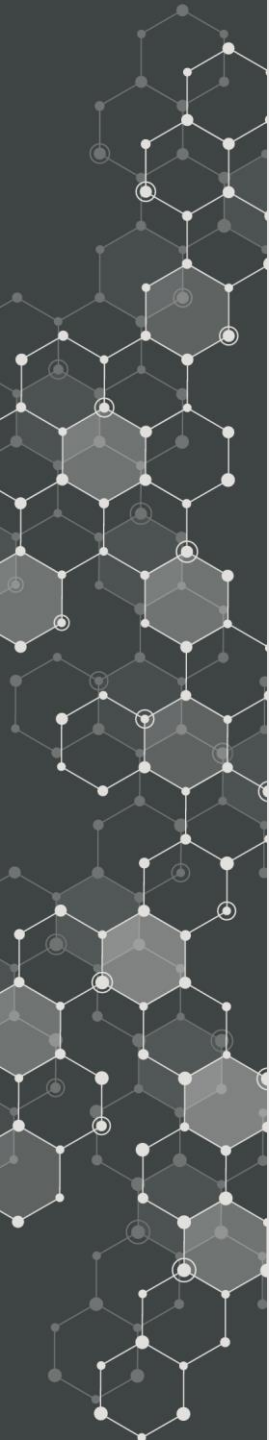


# SHRED MINDSET: HOW TO?

- Ensure that each subgroup, team, or team member feels empowered and valued
  - for their contributions to the team/organization's goals
- Create shared experiences
- "Structured unstructured time"
  - Time blocked off in the schedule to talk about matters not directly related to the tasks at hand



CAL FIRE  
LABS



CALFIRE  
LABS

# TIME MANAGEMENT THROUGH TASK MANAGEMENT



C  A L F I R E  
LABS

# ACCOMPLISH MORE IN SHORTER TIME

- Keep a track of your obligations / tasks
- Set and achieve your short and long term goals
- Assist with multi-tasking
- Reduce and eliminate distractions
- Reduce stress 😊



CAL FIRE  
LABS



# TIME MANAGEMENT THROUGH TASK MANAGEMENT



CAL FIRE  
LABS



# TIME MGMT. THROUGH TASK MGMT.

- Instead of fitting work into 8 hours
  - Think: What tasks I have and how much time per task is required
  - This will force you to say “No” when necessary
- Task management provides us with a sense of accomplishment
- Task management is tangible
  - You can see / communicate your success



CAL FIRE  
LABS

# MULTI-TASKING LIKE A PRO

- Get the big picture
- Sequence strategically
- Protect yourself
  - Set and communicate expectations
  - Document and communicate task status
- Working on a task that requires undivided attention?
  - Set an auto-reply in Outlook/etc. for that time-period



CALFIRE  
LABS

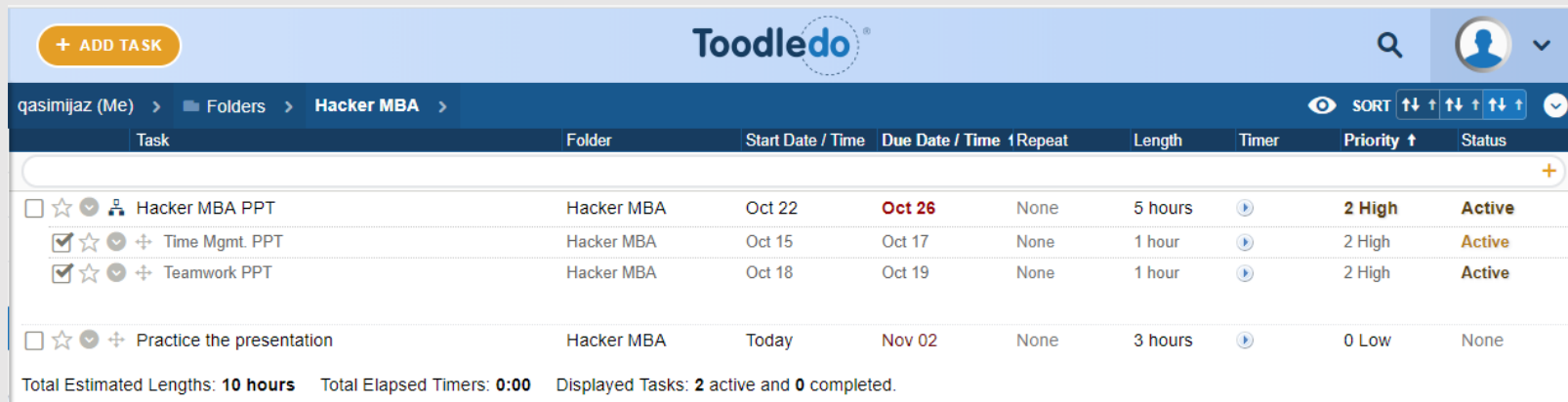
# TASK MANAGEMENT TOOLSET



COAL FIRE  
LABS

# TAMING THE TO-DO LIST

- List-based (Try Wunderlist, Todoist, or Toodledo)
  - Organize by priority or due date
  - Prioritize by
    - Due date
    - Impact on the bigger picture (project)
    - Organizational needs (Context/Dependencies)



The screenshot shows the Toodledo web application interface. At the top, there is a blue header with the 'Toodledo' logo, a search icon, and a user profile icon. Below the header, a breadcrumb trail shows 'qasimijaz (Me) > Folders > Hacker MBA >'. A 'SORT' dropdown menu is visible. The main content area is a table with columns: Task, Folder, Start Date / Time, Due Date / Time, Repeat, Length, Timer, Priority, and Status. The table lists four tasks, with the first three being active and the last one being 'None'. A summary bar at the bottom indicates 'Total Estimated Lengths: 10 hours', 'Total Elapsed Timers: 0:00', and 'Displayed Tasks: 2 active and 0 completed.'

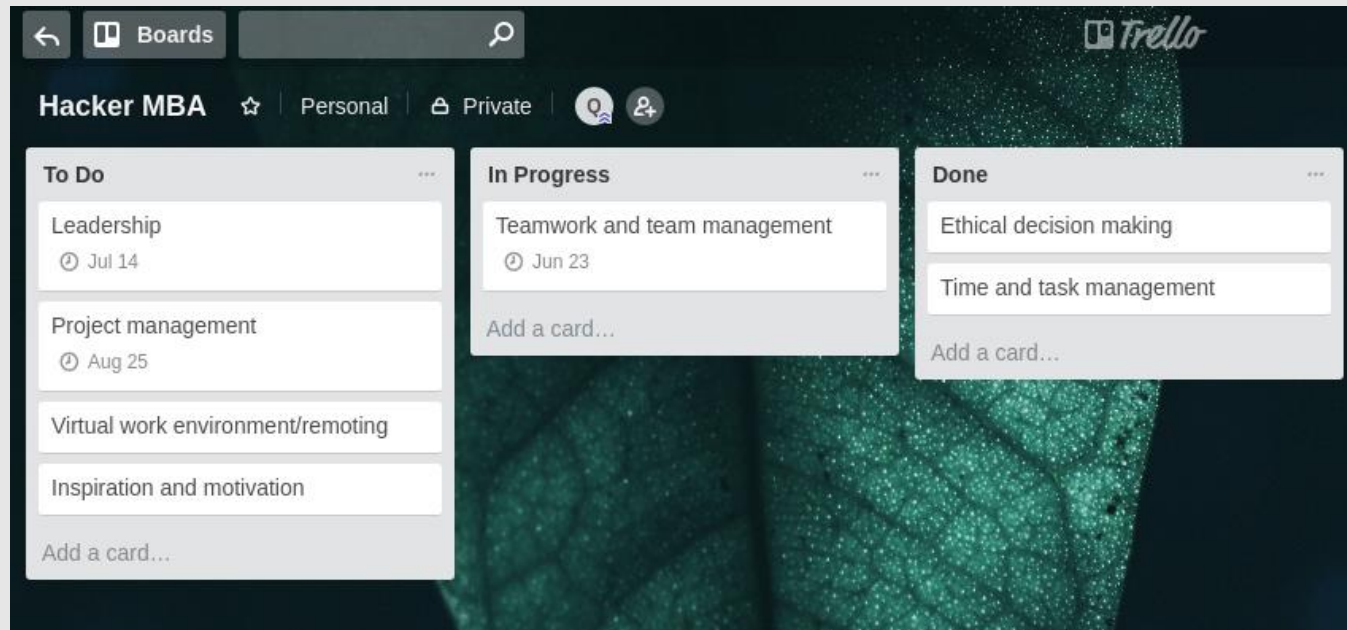
Task	Folder	Start Date / Time	Due Date / Time	Repeat	Length	Timer	Priority	Status
<input type="checkbox"/> Hacker MBA PPT	Hacker MBA	Oct 22	Oct 26	None	5 hours		2 High	Active
<input checked="" type="checkbox"/> Time Mgmt. PPT	Hacker MBA	Oct 15	Oct 17	None	1 hour		2 High	Active
<input checked="" type="checkbox"/> Teamwork PPT	Hacker MBA	Oct 18	Oct 19	None	1 hour		2 High	Active
<input type="checkbox"/> Practice the presentation	Hacker MBA	Today	Nov 02	None	3 hours		0 Low	None

Total Estimated Lengths: 10 hours   Total Elapsed Timers: 0:00   Displayed Tasks: 2 active and 0 completed.



# TAMING THE TO-DO LIST

- Kanban (try Trello)
  - Card/sticky-note based task management
  - Categorize tasks
    - To Do, In Progress, Done



# FOR THE FAINT OF HEART: COMMAND LINE TO-DO LIST

- `sudo apt install taskwarrior`
  - `sudo yum install task`
  - `pacman -S task`
  - <https://taskwarrior.org/download>
- Other options: <http://todolist.site> and <http://todotxt.com>

```
q@DELL:~$ task next
```

<u>ID</u>	<u>Age</u>	<u>Due</u>	<u>Description</u>	<u>Urg</u>
2	2min	12h	--project:Coalfire Create Pentest report	8.55
3	11s	6d	Submit timesheet	5.6
1	12min		Prepare Time and Task Mgmt PPT due:Friday	0



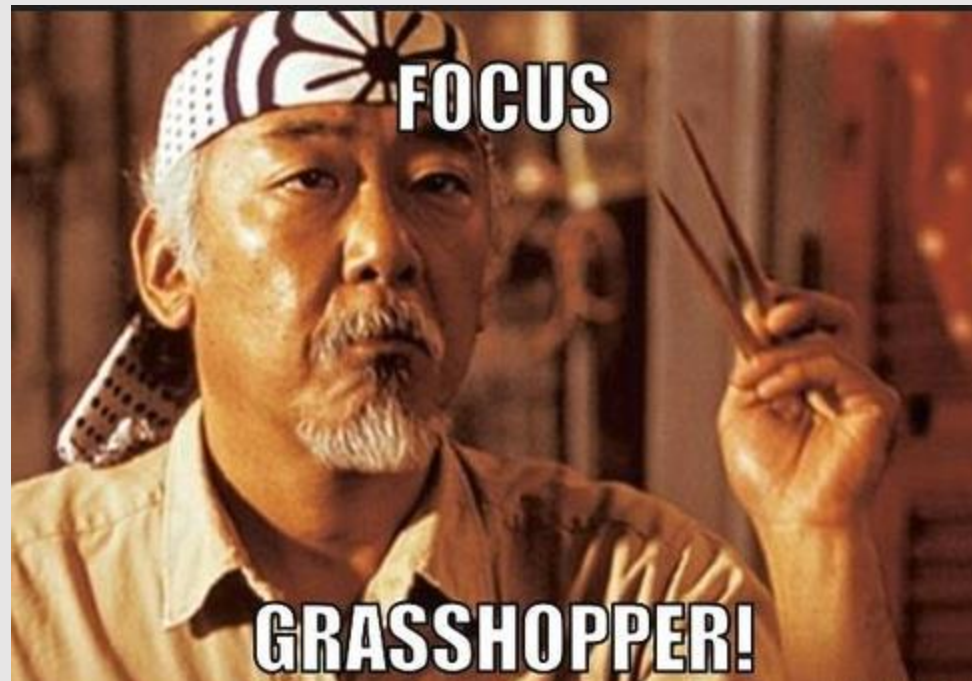
COALFIRE  
LABS



Make your to-do list/app work for you



CALFIRE  
LABS



# PRO TIP: DELEGATION AND NOT-TO-DO LIST

- Ask yourself how each task already on the list does not contribute to your goals
  - Does this task really need to be done?
    - If yes, does it really need to be done by you?
      - If no, then delegate
    - If no, create a not-to-do list
      - I call it "Sometime in the future" list
      - Any tasks that don't need to be done in near future, go here
- This is liberating :)



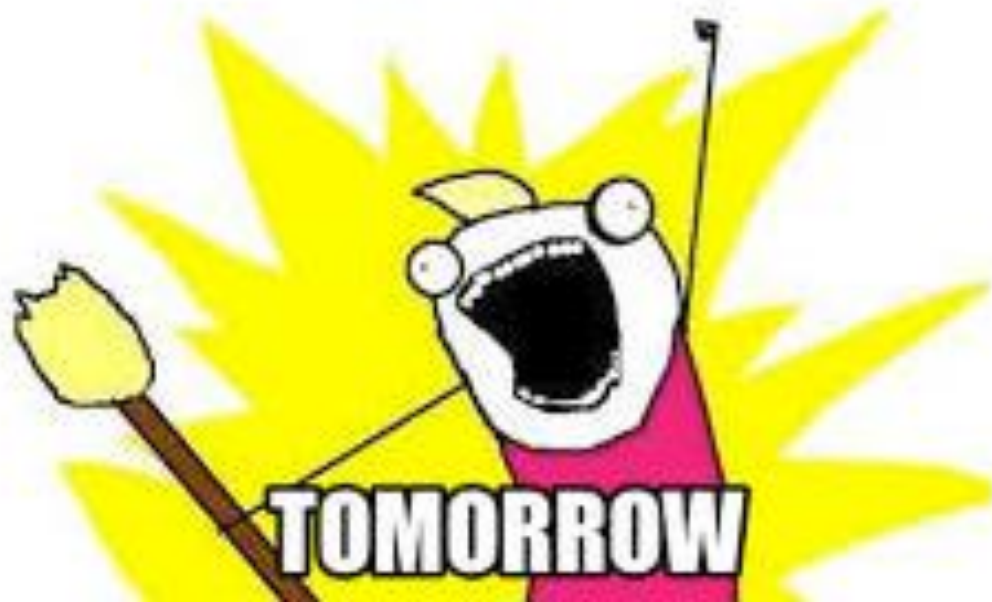
C O A L F I R E  
LABS

Regain Your Sense of Control by  
checking off a "Done today" list  
of accomplishments



COAL FIRE  
LABS

**DO ALL THE THINGS**



**TOMORROW**

# PROCRASTINATION IS

“Purely a visceral (primitive), emotional reaction to something we don’t want to do”

Tim Pychyl – author of *“Solving the Procrastination Puzzle”*



COAL FIRE  
LABS



# BEAT PROCRASTINATION

- Seven triggers – reverse them!
  1. Boring
  2. Frustrating
  3. Difficult
  4. Ambiguous
  5. Unstructured
  6. Not essentially rewarding
  7. Lacking in personal meaning
- Do Something!



CAL FIRE  
LABS

# HACKER



What my friends think I do



What my Mom thinks I do



What society thinks I do



What the government thinks I do



What I think I do

```
felix@map:~$ nmap -iL 14 scanme.nmap.org

Starting nmap 3.75 ( http://www.insecure.org/nmap/ ) at 2004-10-26 11:31 PDT
Interesting ports on scanme.nmap.org (205.227.153.95):
(The 1550 ports scanned but not shown below are in state: filtered)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 3.1p1 (protocol 1.99)
25/tcp    open  smtp     postfix
53/tcp    open  domain   ISC BIND 9.2.1
80/tcp    open  http     Apache/2.0.33 ((Ubuntu) mod_per/1.99_0-dev Perl/4.5.6,1)
113/tcp   closed auth
Device type: general purpose
Running: Linux 2.4.302.5.X
OS details: Linux 2.4.0 - 2.5.20, Linux 2.4.18 - 2.4.20
Uptime: 236,991 days (since Mon Apr 12 22:18:53 2004)

Nmap run completed -- 1 IP address (1 host up) scanned in 27.003 seconds
felix@
```

What I actually do



# ETHICAL DECISION MAKING



C  A L F I R E  
LABS



**"ETHICAL HACKER"**

[memegenerator.net](http://memegenerator.net)



COAL FIRE  
LABS

# WHY “ETHICAL” HACKING: NO RIGHT OR WRONG ANSWERS

- Do you do the right thing for the client (whole company) or their staff (individual)
  - Do you report the names of individuals who fell for social engineering?
    - What if its their first job and first day on the job?
- Do you stick with specific scope even if a Windows Server 2000 box has open RDP port outside of your external network scope?
- In heat of the moment, Associate Consultant, first day on the job, kicks off a Nessus scan against a segment outside the scope of the engagement
  - How do you report this incident to the client?
  - Who takes the responsibility?

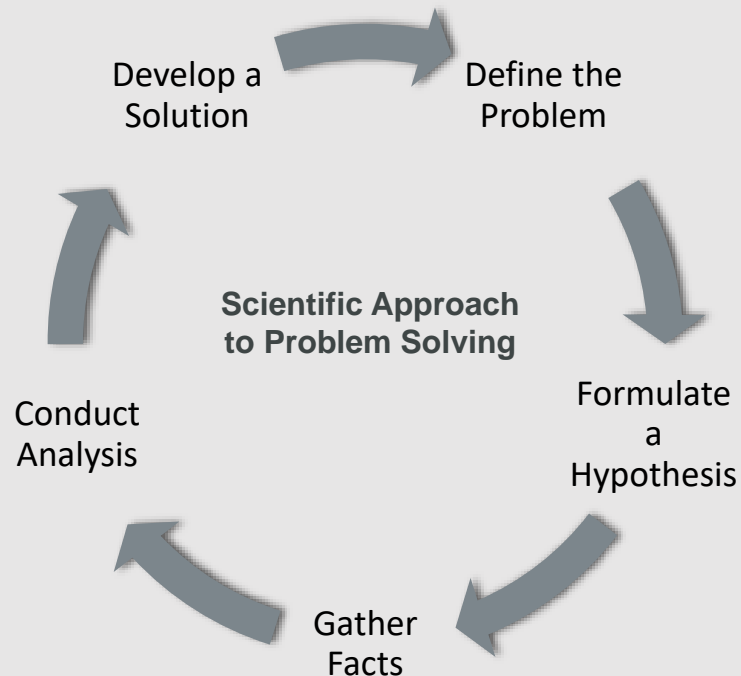


CAL FIRE  
LABS



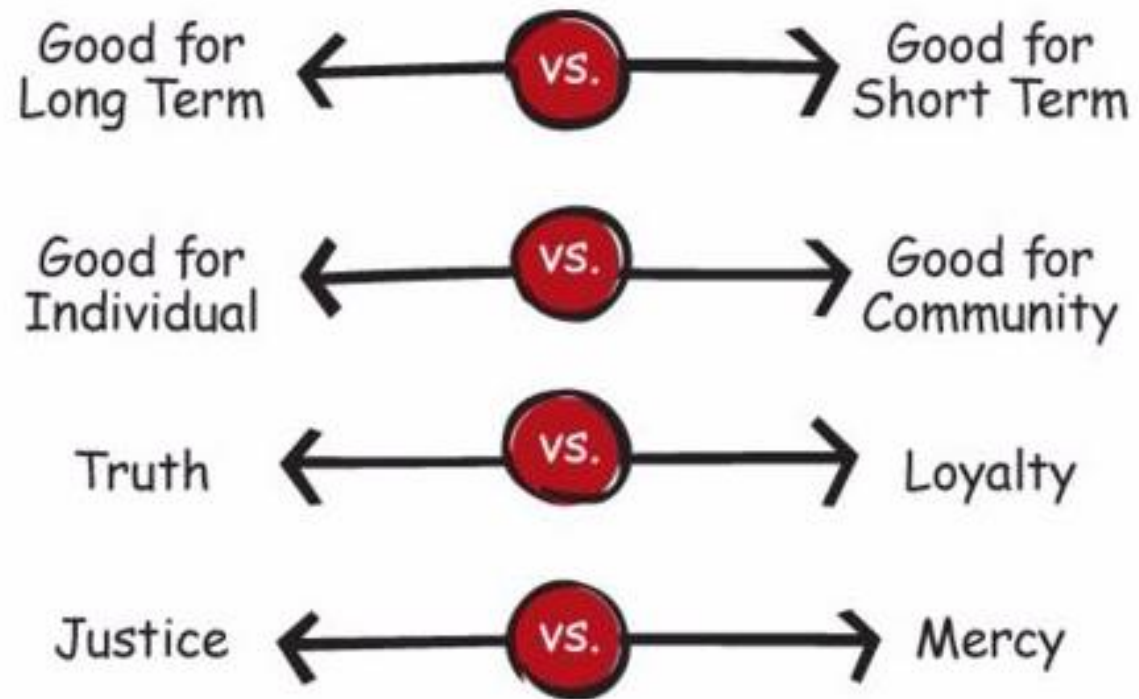
# SOLVING RIGHT VS. WRONG

- Can be solved using scientific approach to problem solving
- Artifacts from a previous possible breach found on client systems
- Teammate stealing sensitive data from client systems and selling it to APT 28





# RIGHT VS. RIGHT



COAL FIRE  
LABS

# 4 STEPS TO ETHICAL DECISION MAKING

1. Pick a plan that does most good and least harm
  - a.k.a Utilitarianism
2. Does it best serve other's rights, including shareholders' rights?
3. Can I live with it? Is it consistent with our basic values and commitments?
4. Is it feasible in the world as it is?



CAL FIRE  
LABS

# LEADERSHIP THROUGH EXTREME OWNERSHIP



# LEADERSHIP

- Everyone here is a leader
  - Engagement Leads
  - Mentors
  - Researcher or blog post writer
    - Leading a team of 1 or many
- There are no bad teams
  - There may be challenging teams
- Lead by example
  - “Let me show you how to do it efficiently”
- Inspire, don't require
  - Don't be Bill Lumbergh



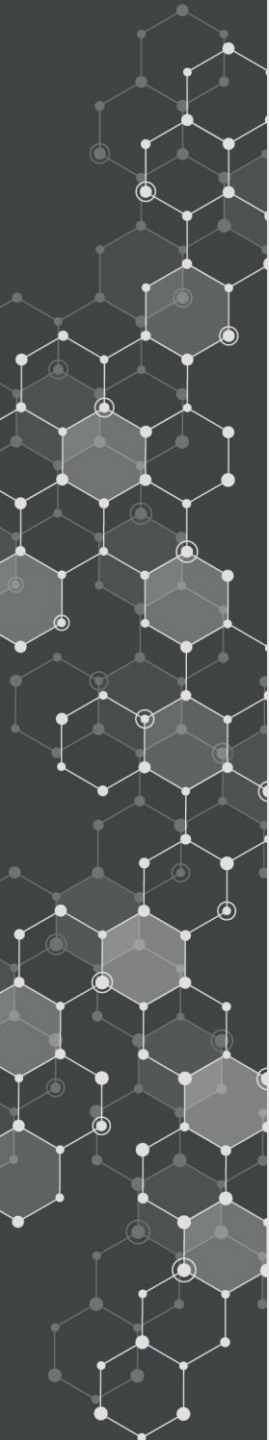
CALFIRE  
LABS

# EXTREME OWNERSHIP

- Explain the “Why” behind the decision
- Get good at “information sharing”
  - Communicate upward and downward
- “Prioritize and execute”
  - Not all problems require the same priority
    - Delegate when you don’t need to know personally
  - But avoid “Improvement overload”
- Keep it simple
  - Avoid complexity like a plague!



CAL FIRE  
LABS





# EFFECTIVE WRITTEN & VERBAL COMMUNICATION



COAL FIRE  
LABS

# EMAIL COMMUNICATION

- Avoid contracted forms
  - Do not > don't
  - We'll < We will
- Provide context
  - Don't just assume the recipient knows what you are talking about
- Provide detail but avoid verbosity (-v > -vvv)
  - Use bullet points where necessary
- Start the email with important information
- Title says it all
  - Subject: Please Respond – Change of Scope
- Email == FYI
  - Call == I need this urgently



CALFIRE  
LABS

# CONFERENCE CALLS

- Let the organizer know if you cannot attend
  - Have a good reason if it's a client call
- For client calls
  - Review any documents beforehand
  - Write down questions or bullet points you'll need to discuss
  - Be semi-formal
  - Use the "Mute" button 😊
- Use an Agenda!
  - Every call has a "leader"
  - The call lead (e.g. PM) should ensure every topic gets its due time



CALFIRE  
LABS

# THANKS

TWITTER: @HASHTAGINFOSEC



COAL FIRE  
LABS