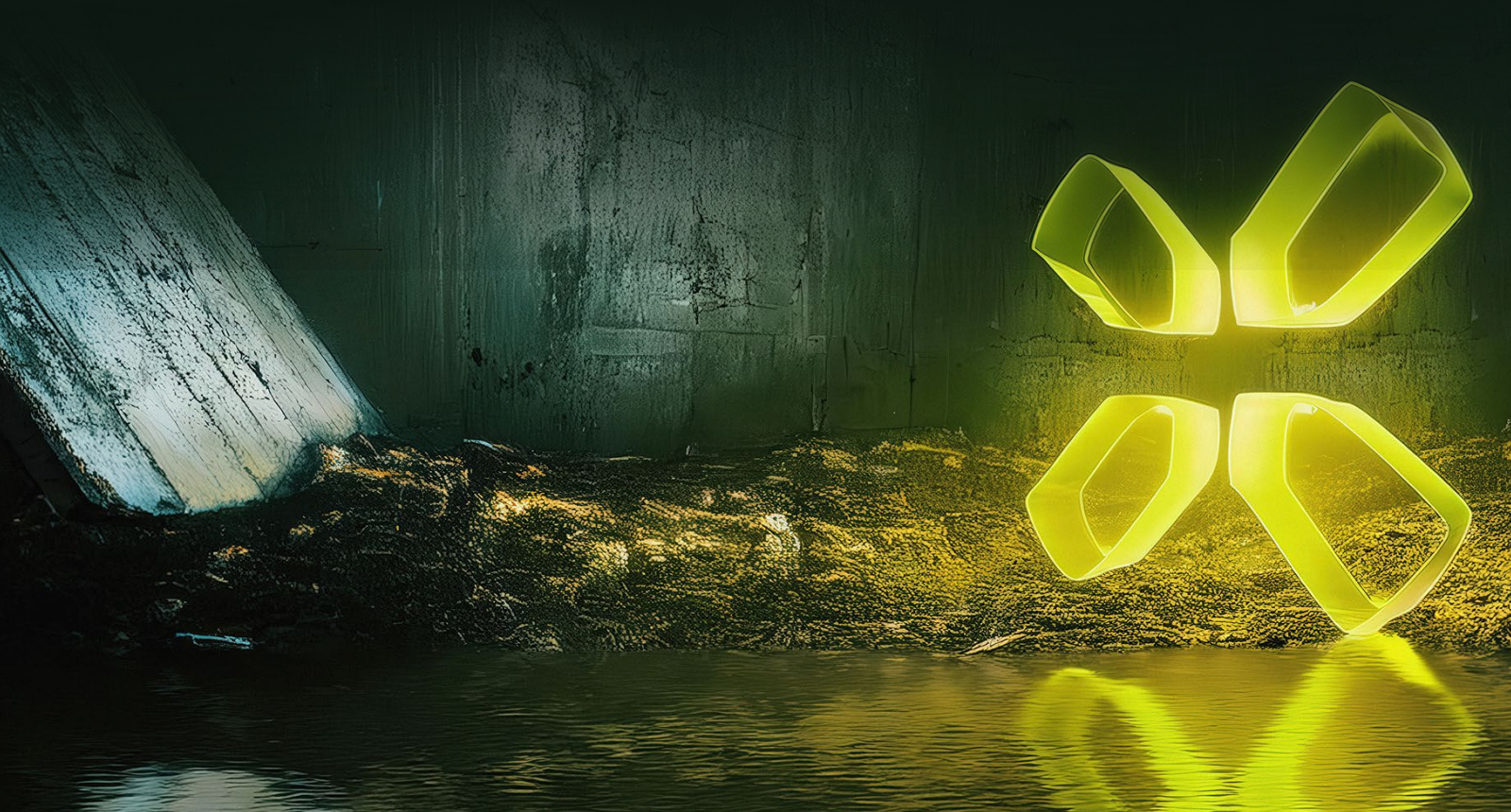
Mind Science

RANGE FORCE

SOFT SKILLS FOR HARD JOBS

The CREW Framework - Measuring teamwork in cybersecurity incident response



OVERVIEW

AN INTRO FROM MINDSCIENCE FOUNDER, REBECCA MCKEOWN

The important role teamwork plays in successfully navigating high pressure situations is well known. Sports teams, emergency services, the military and more have all established approaches to building soft skills. They know that by honing interpersonal capabilities such as communication and leadership, individuals become more than the sum of their parts when called upon.

Teamwork is just as important in cybersecurity defense. Unfortunately, an intangible asset in an otherwise highly tangible environment, soft skills often come second place to individual technical ones. Lacking definition, categorization and measurement, security leaders struggle to incorporate their development into strategies and budgets, despite having an innate understanding of their importance.

Rebecca McKeown, an academic and psychologist with 20+ years of experience, specializes in high-performing teams in defense and cybersecurity. She now leads MindScience.

View Rebecca's full profile on mindscienceltd.co.uk >

The CREW framework is an attempt to redress this balance by bringing structure, clarity and measurement to the soft skills used in incident response.

A free framework for using alongside team exercises, it highlights the 4 core competencies and 12 contributing behaviours necessary for a high performing defensive cyber team. It presents these in an accessible format so they can be scored, assessed and, used regularly, matured over time.

While underpinned by detailed research - the goal was to build an open and pragmatic schema that can be picked up and used quickly and easily. In a time precious sector awash with complex frameworks, we wanted to remove barriers to usage. In keeping with this ethos, this document also provides a walk-through on how to use it, and access to templates for the accompanying assets needed to track performance during an exercise.

THE CREW FRAMEWORK

The framework splits soft skills in cybersecurity incident response into four key competencies. These are the core behavioural, cognitive, and emotional attributes which should underpin a high performing defensive team.

Each competency is made up of three constituent behaviours, as outlined in the framework below. These behaviors act as an umbrella term, bringing together related soft skills typically exhibited in an incident.

Defining individual behaviors is important in the context of the framework. It actualizes something which, until this point, has largely existed in the abstract. With a label, soft skills become measurable.

Competency	Collaboration	Resilience	Evaluation	Workflow
Behavior	Communication clarity	Stress management	Problem solving	Role clarity
Behavior	Information sharing	Conflict resolution	Situational awareness	Task allocation
Behavior	Mutual support	Recovery	Adaptability	Protocol adherence

Fig. 1 The CREW Framework

The table below describes an ideal state for each behavior. This provides a yardstick for comparison when seeking to analyse the efficacy of a team's soft skills.

By understanding how closely each behavior is to the ideal state, we can score strengths and weaknesses. By observing how well competencies and behaviors interact throughout an incident, we get an overall picture of teamwork.

Competency	Behavior	Ideal State
Collaboration	Communication clarity	Messages are clear, concise and understood by recipients
	Information sharing	Relevant data is shared promptly with appropriate stakeholders
	Mutual support	Team members proactively assist others facing challenges
Resilience	Stress management	Maintains composure under pressure and manages stress constructively
	Conflict resolution	Addresses disagreements or friction constructively and promptly
	Recovery	Quickly regroups after setbacks to resume efficient operations
Evaluation	Problem solving	Effective identification and prioritisation of key issues
	Situational awareness	Demonstrates understanding of the broader threat landscape
	Adaptability	Adjusts strategies effectively in response to evolving situations
Workflow	Role clarity	Team members demonstrate understanding and execution of their roles
	Task allocation	Tasks are appropriately distributed to leverage expertise
	Protocol adherence	Actions align with pre-established response frameworks

Fig 2. CREW Framework's behaviour descriptors

USING THE CREW FRAMEWORK

Environment

The framework is designed to ensure consistent, objective and actionable assessment of teamwork by an observer of a team cybersecurity exercise.

Such exercises typically take place in a range which allows for the approximate replication of attack conditions. Factors such as real tools, networks, time pressures, processes and attack chains enable the faithful testing of team behaviours. The type of attack being run should also reflect the risk profile of the organization being assessed. However, building a resource-consuming exact replica of the participants' technical environment is not necessary.

Guide

1. PREPARE

a. An observer should be selected, this is usually the sponsor of the exercise - typically the SOC Manager or similar. They should have access to all exercise communications and actions, virtual or in-person.
b. Observers will prepare for the exercise by familiarising themselves with the team's individual roles, team objectives and protocols.
c. It is useful for observers to have access to the following assets:
    i. A notepad / electronic device to make notes
    ii. CREW Framework data capture sheet
    iii. CREW Framework scoring guidelines sheet

2. OBSERVE

a. Data collection starts at the beginning of the team exercise.
b. The observer watches for the behaviours detailed in the framework as they happen.
c. Observation relies on objectivity. It's also crucial to remain unobtrusive to avoid influencing participants' behaviour.
d. Only observable actions are relevant, not assumptions.

3. RECORD

a. The observer systematically documents examples of the behaviours observed.
b. It is important to note the people involved for later evaluation.

c. For data capture:

i. If capturing notes on a notepad or in written format - write the competency area, followed by the behaviour code and note what happens, followed by who was involved. For example if you see a participant behaviour related to information sharing, this should recorded and marked as ‘A2’.

Competency	Behavior	5 - Exceptional	4 - Exceeds expectations	3 - Meets expectations	2 - Below expectations	1 - Poor
A. Collaboration	1. Clarity of Communication	Always clear, concise, and checks for understanding.	Clear but occasionally misses minor details.	Generally clear but may lack precision.	Communication sometimes unclear or incomplete.	Frequently vague or confusing.
	2. Information Sharing	Proactively and promptly shares critical info.	Regularly shares relevant info without prompting.	Shares info when asked.	Shares info inconsistently or late.	Withholds or delays sharing info.
	3. Mutual Support	Proactively assists teammates without prompting.	Offers support frequently.	Helps when asked but rarely initiates.	Occasionally ignores others’ struggles.	Ignores or refuses to help others.

ii. If using the CREW framework data capture sheet, simply mark the observed behaviour in the relevant area. With this asset, you can score as you work.

d. If you did not observe any of the behaviours, then record it as ‘no evidence’.

e. Make a note of any patterns or trends you notice throughout the exercise. You can also identify strengths and development needs. These will be useful discussion points for the debrief.

4. CLASSIFY

a. Once recorded, a team’s behaviours need to be given a final score.

b. Ratings are on a 5-point Likert scale with specific behavioural anchors to guide observers. This ensures the scores given are fair, accurate and consistent.

c. Detailed guidance on scoring can be found in the separate CREW Framework Scoring guidelines. An overview is also in the appendix of this document.

d. Scores are intended to act as overall ratings for the exercise, so consult the notes you took during the exercise before deciding.

e. Avoid half point scores, which can insert ambiguity.

5. EVALUATE

a. In this final stage, the observer assesses the data for patterns and trends with the aim of identifying strengths and development needs.

b. This should be included in the post exercise wash-up, supported by the evidence of observed behaviours.

SCORING GUIDANCE

Collaboration

Clarity of communication

Rating	Behavior
5 - Exceptional	Consistently communicates clearly and concisely, confirming understanding and encouraging feedback.
3 - Meets expectations	Provides mostly clear communication but occasionally omits important details or fails to check for understanding.
1 - Poor	Frequently communicates unclearly or ambiguously, causing confusion and errors.

Information Sharing

Rating	Behavior
5 - Exceptional	Proactively and promptly shares critical information without prompting, ensuring team alignment.
3 - Meets expectations	Shares necessary information when asked but rarely volunteers updates or insights.
1 - Poor	Withholds or delays sharing important information, leading to gaps in response efforts.

Mutual Support

Rating	Behavior
5 - Exceptional	Actively monitors the team and offers help without being asked, fostering collaboration.
3 - Meets expectations	Offers assistance when requested but does not consistently seek opportunities to support others.
1 - Poor	Ignores or is unaware of teammates struggling, focusing only on personal tasks.

Resilience

Stress Management

Rating	Behavior
5 - Exceptional	Remains calm, focused, and supportive, positively influencing team morale.
3 - Meets expectations	Generally composed but shows signs of stress during peak moments.
1 - Poor	Visibly overwhelmed, causing disruption or anxiety within the team.

Conflict Resolution

Rating	Behavior
5 - Exceptional	Proactively resolves conflict through open discussion, fostering team cohesion.
3 - Meets expectations	Addresses conflict when necessary but may avoid confrontation or resolution
1 - Poor	Ignores or escalates conflicts, negatively affecting team performance.

Recovery

Rating	Behavior
5 - Exceptional	Rapidly recovers from setbacks, refocusing the team and driving progress.
3 - Meets expectations	Recovers after setbacks but may need time or support to regain focus.
1 - Poor	Struggles to recover, resulting in prolonged disruption and reduced performance.

SCORING GUIDANCE

Evaluation

Problem solving

Rating	Behavior
5 - Exceptional	Quickly identifies core problems, prioritises actions effectively, and proposes solutions.
3 - Meets expectations	Identifies and solves problems but may need guidance for complex issues.
1 - Poor	Struggles to identify critical issues, leading to ineffective solutions or delays.

Situational Awareness

Rating	Behavior
5 - Exceptional	Maintains full awareness of evolving threats and integrates new information into response actions.
3 - Meets expectations	Recognises immediate threats but may miss broader or emerging risks.
1 - Poor	Lacks awareness of the overall threat environment, leading to reactive decision-making.

Adaptability

Rating	Behavior
5 - Exceptional	Quickly and effectively adapts strategies to changing conditions without sacrificing performance.
3 - Meets expectations	Adapts when necessary but may require prompting or additional time.
1 - Poor	Struggles to adjust plans, persisting with ineffective strategies.

SCORING GUIDANCE

Workflow

Role Clarity

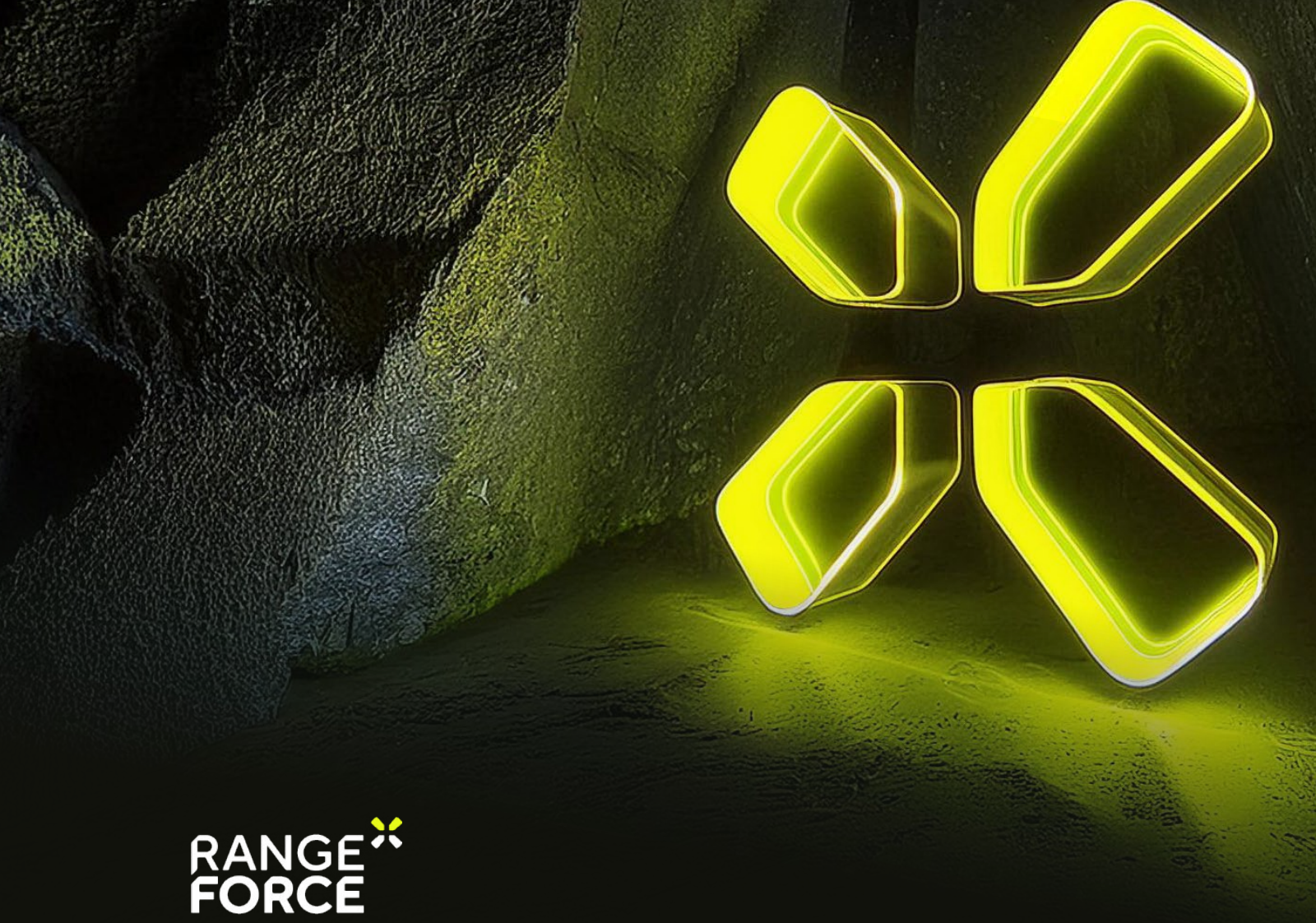
Rating	Behavior
5 - Exceptional	Fully understands and performs assigned roles while ensuring others are aligned with theirs.
3 - Meets expectations	Generally understands their role but occasionally overlaps tasks or needs clarification.
1 - Poor	Appears unclear about their role, causing confusion or duplication of work.

Task allocation

Rating	Behavior
5 - Exceptional	Delegates tasks strategically based on skills and workload, balancing responsibilities effectively.
3 - Meets expectations	Assigns tasks adequately but may not fully leverage the team's strengths.
1 - Poor	Fails to distribute tasks effectively, leading to bottlenecks or underutilized resources.

Protocol adherence

Rating	Behavior
5 - Exceptional	Consistently follows response protocols and adapts them appropriately when necessary.
3 - Meets expectations	Generally follows protocols but occasionally requires reminders or clarification.
1 - Poor	Frequently disregards or misunderstands response protocols, leading to procedural errors.



RANGE FORCE

Originally built for NATO, RangeForce's cloud-based range is now used to develop high performing defensive teams at organizations worth trillions of dollars.

Test your team against a real attack, using real tools, in a real environment with a free exercise here.

Mind Science

Mind Science's Agile Cyber Crisis Response Programme uses scientific research to improve unit cohesion and decision making.

Mature cyber crisis response capabilities across technical, Communications, GRC and Executive teams by embedding mental agility. Find out more here.