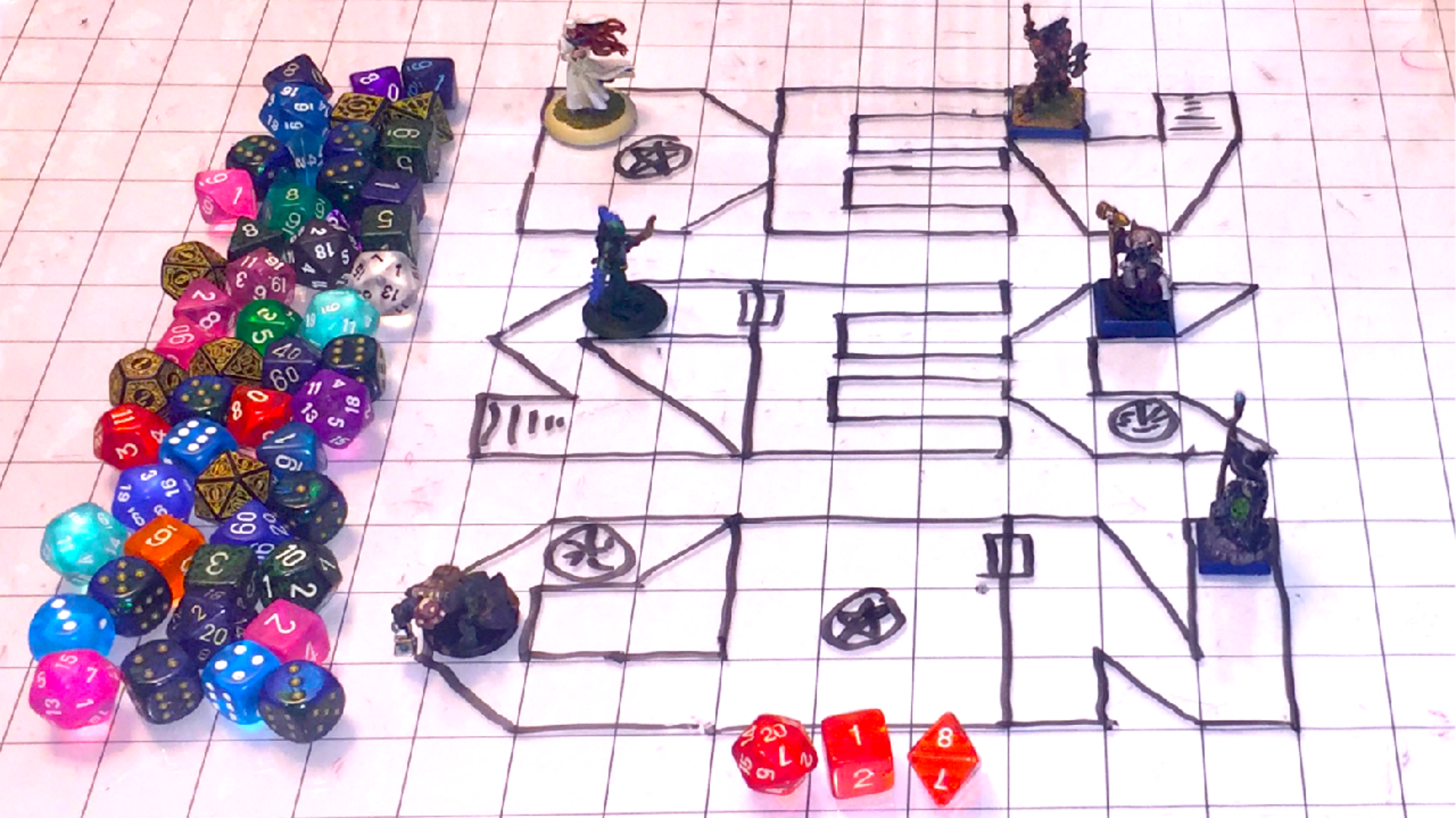
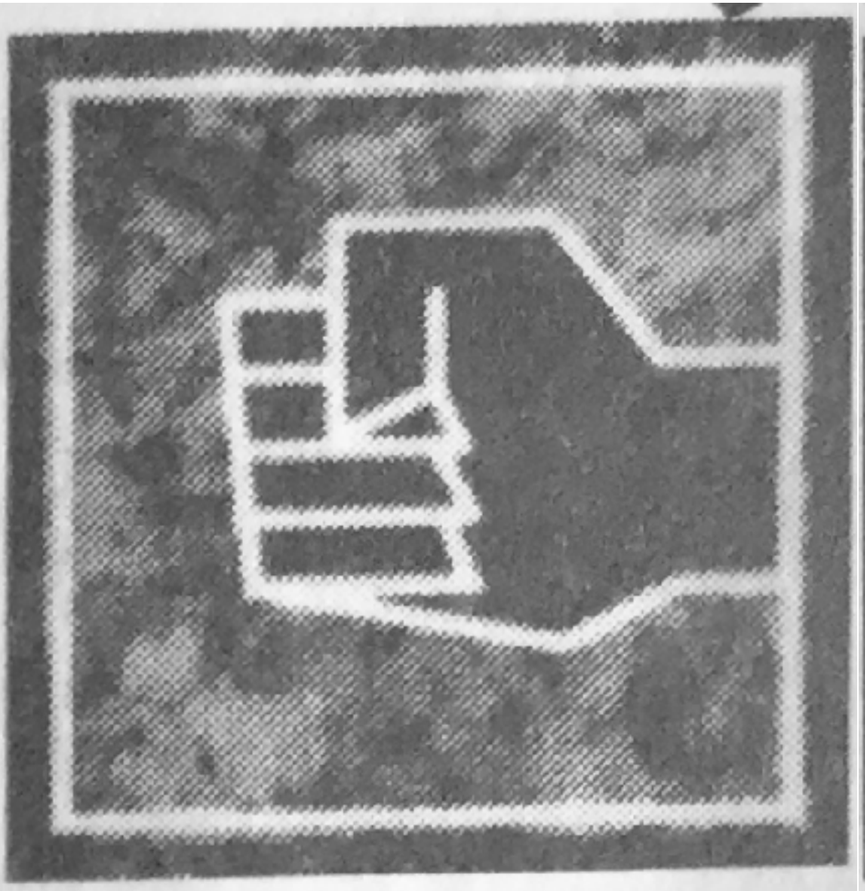
DevSecCon

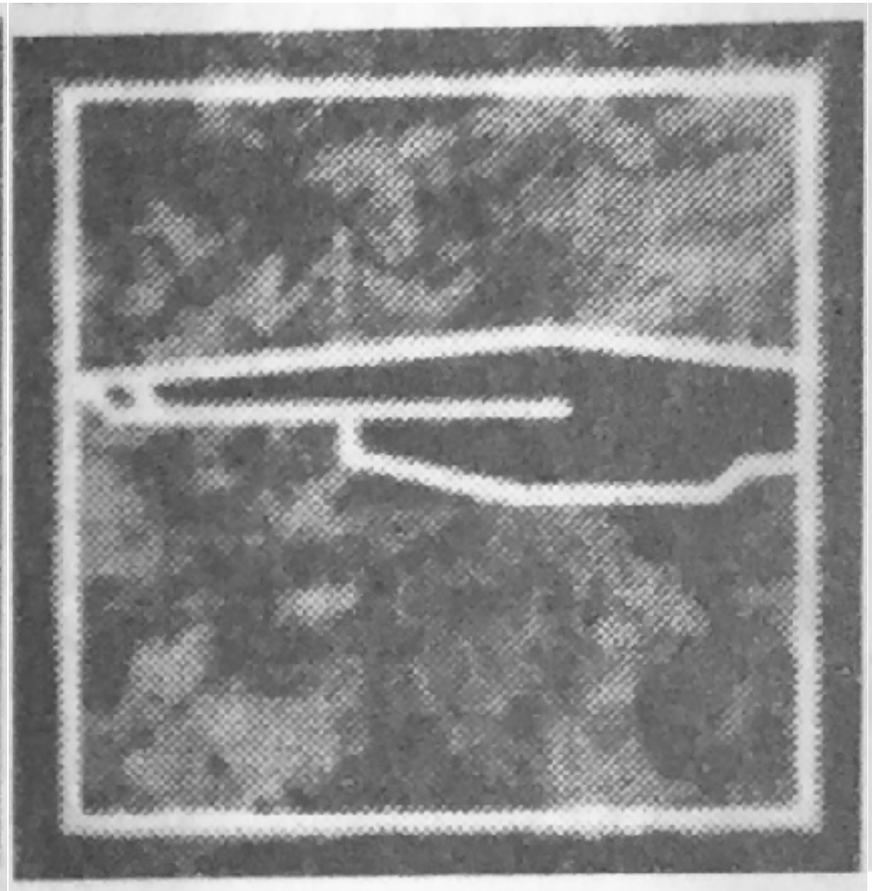
Building Effective DevSecOps Teams Through Role-Playing Games

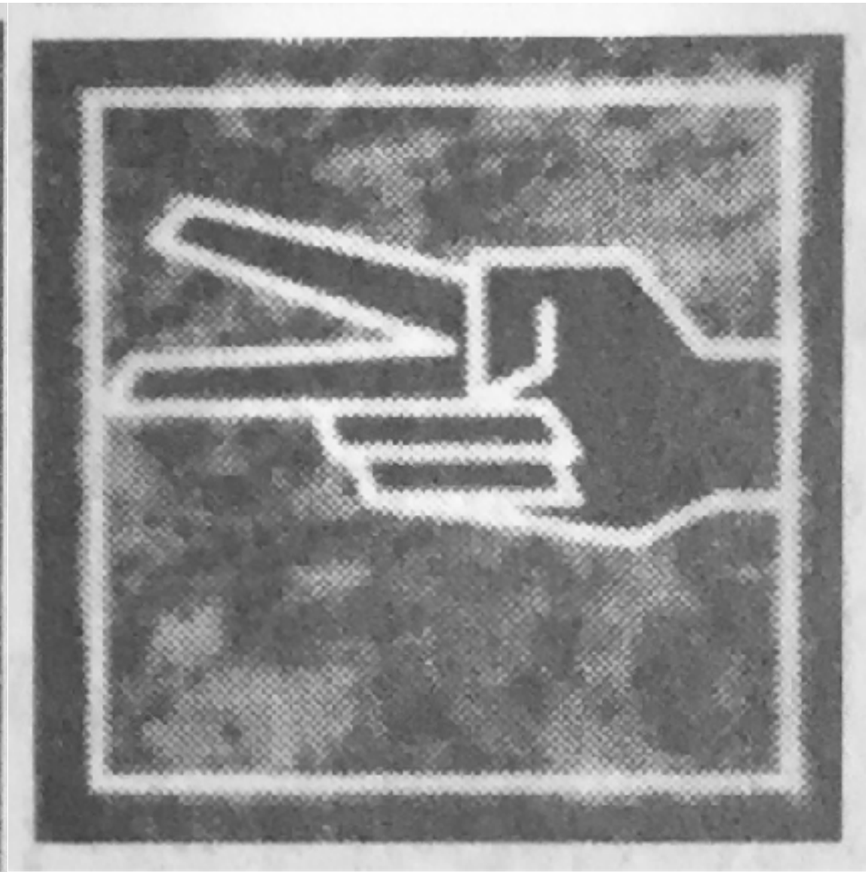
Mike Shema
@CodexWebSecurum

LONDON 18-19 OCT 2018









The Masquerade: Second Edition. White Wolf Game Studio. 1997.

Monstrously Manual

As we treat infrastructure as code and make code more human-readable, we must still find ways to read humans.

DevOps

Automation	Required to scale.
	Establishes consistency.
	Enables confident iteration.

Dev[Sec]Ops

People

Working with them.

Working for them.

Building for them.

Actual Problem Ignored

Users are stupid.

Devs are lazy.

Vuln equals risk.

USENIX Te al Program - Abstract - Security Symposiu 99

Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0

Alma Whitten, *Carnegie Mellon University*; and J. D. Tygar *University of California, Berkeley*

https://www.usenix.org/legacy/publications/library/proceedings/sec99/whitten.html

Fantasy Campaign Setting

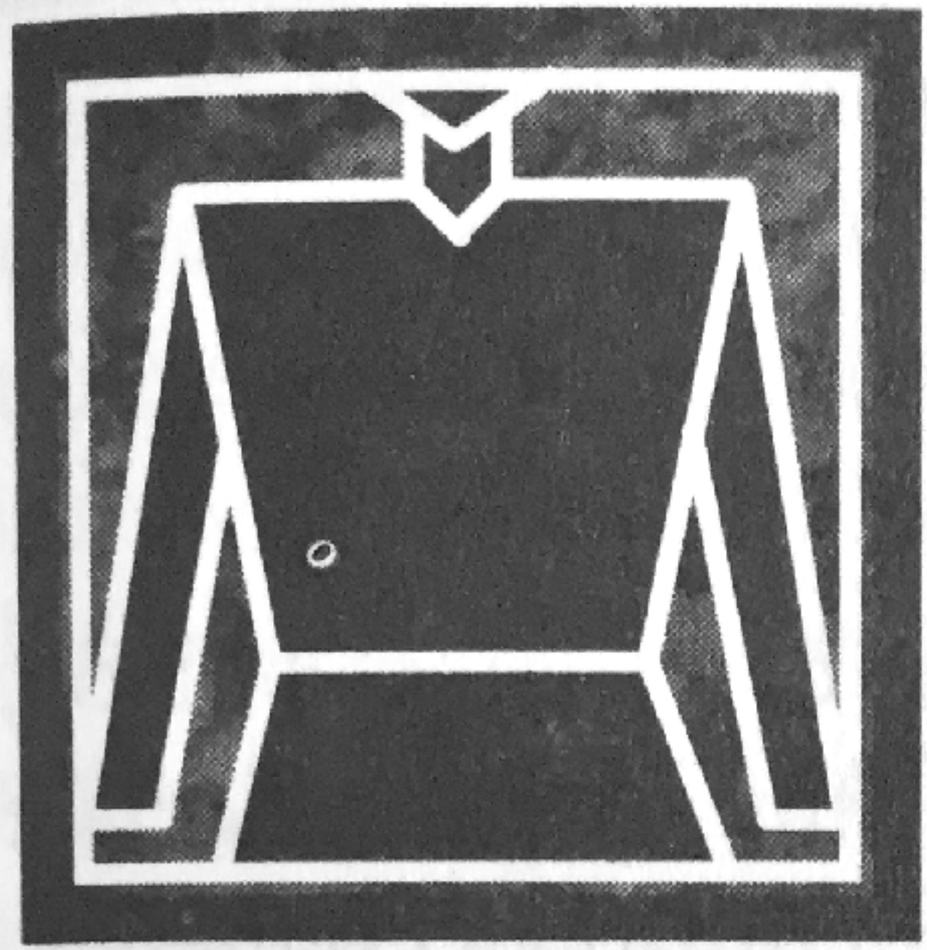
Race	Penalty or Bonus
Dwarf	Constitution +1; Charisma -1
Elf	Dexterity +1; Constitution -1
Half-Orc	Strength +1; Constitution +1; Charisma -2
Halfling	Strength -1; Dexterity +1
User	Intelligence -2; Wisdom -2
Developer	Intelligence -2; Wisdom -2

Collaborative story-telling

Shared goals

Communication exercises

Barbarian	Coder, Sysadmin
Fighter	DevOps
Magic-User	DevOps at scale
Thief	Red Team
Cleric	Blue Team
Ranger	Threat Hunting
Bard	CISO



Advanced

Majesty

You exude an aura of power and insurmountable might. Those around you find it difficult to think about, let alone act out, offenses against your person. You can expect to be treated with great respect, if not awe.

The Masquerade: Second Edition. White Wolf Game Studio. 1997.

Shared Vocabulary

Communication

Empathy

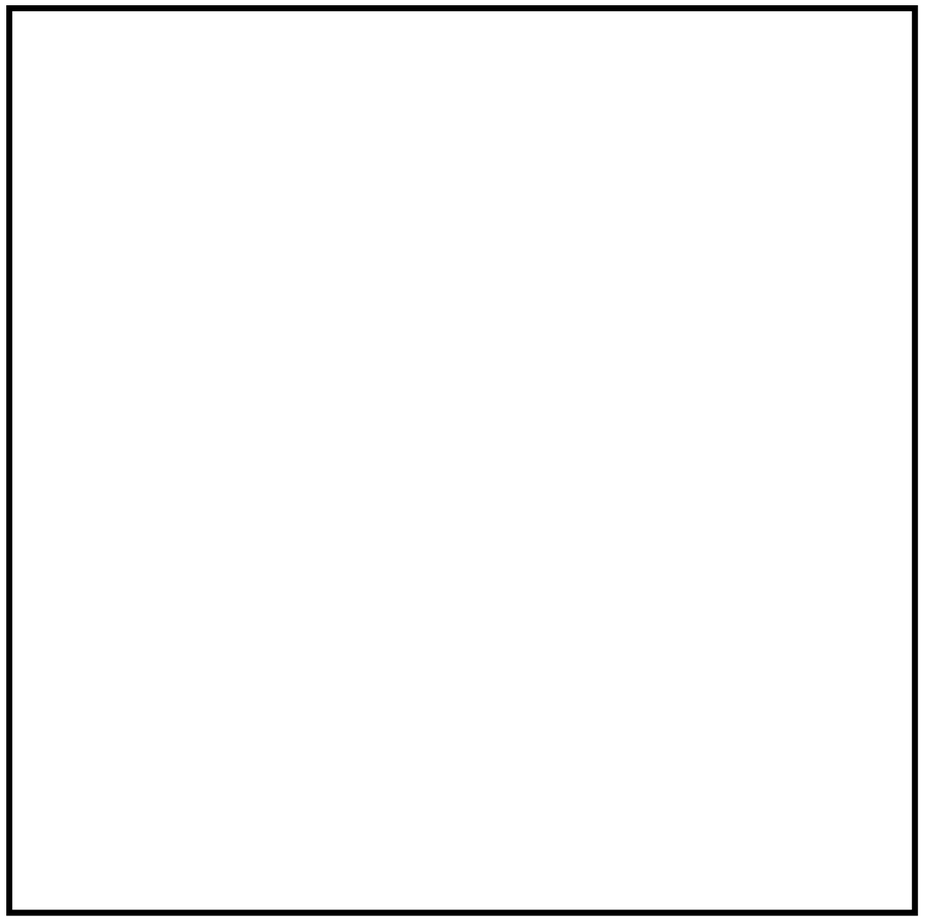
Threats

Communication

Listen

Acknowledge

Repeat back



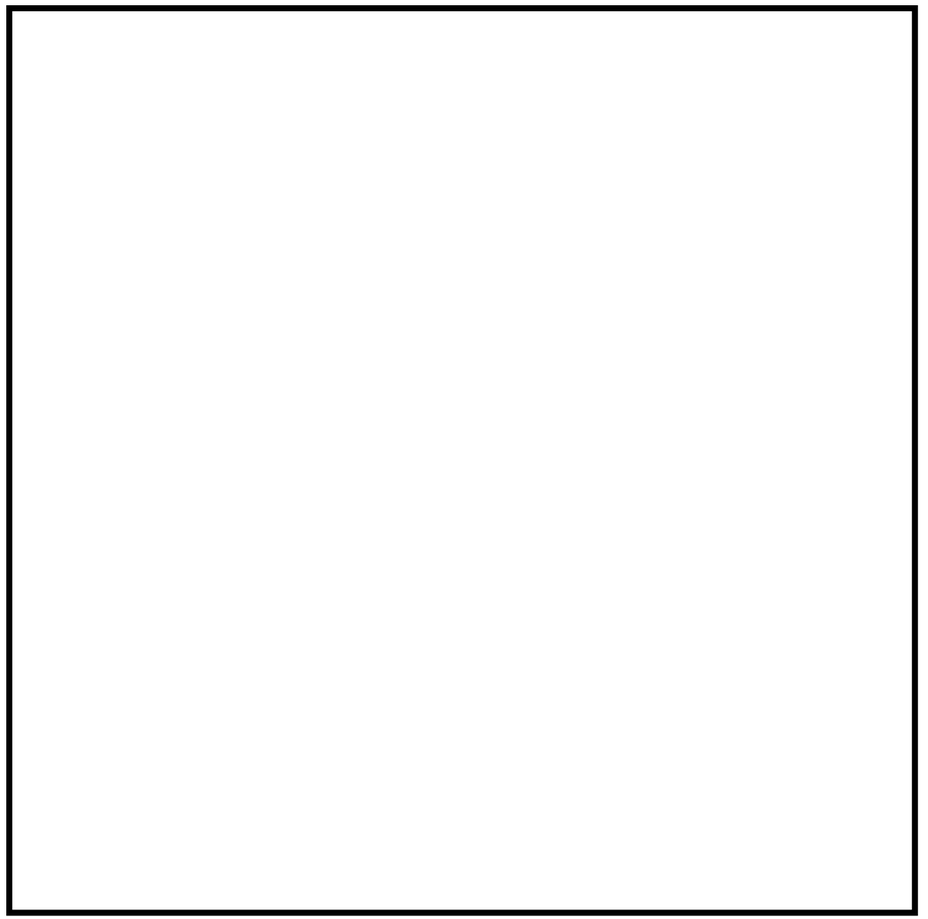
Empathy

Broaden understanding

Reconsider viewpoints

Improve solutions

Constructive feedback



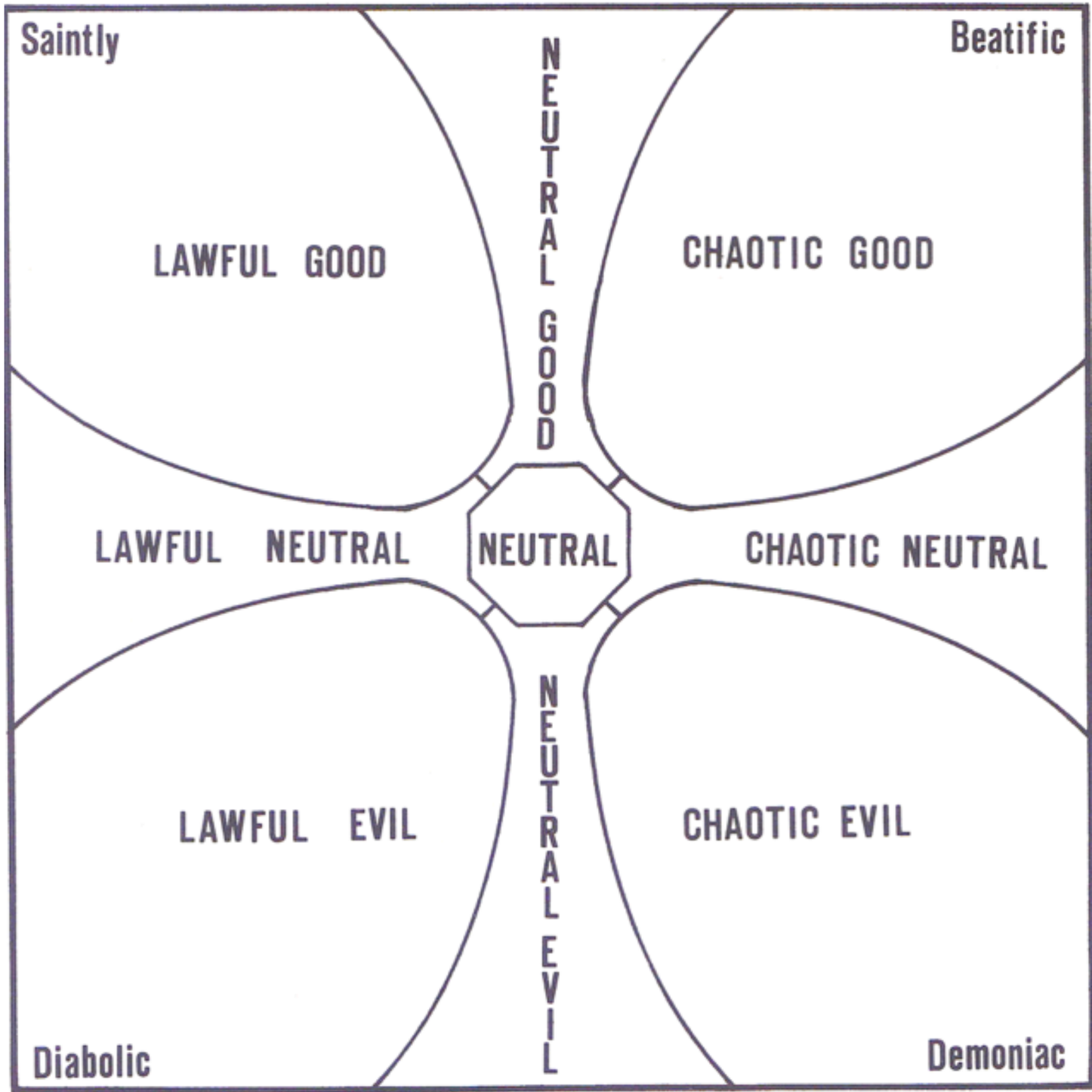
Threats

Ambiguity

Blame

Erasure

Essentialing



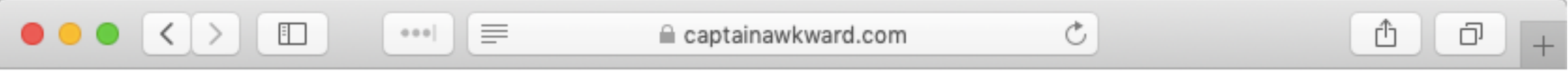
Codes of Conduct

Set expectations, standards of behavior.

Describe a path for conflict resolution, define consequences.

Foster participation.

Example: https://golang.org/conduct



Captain Awkward

Advice. Staircase Wit. Faux Pas. Movies.

Home / About / Archives / Ask a Question / Captain Awkward Elsewhere / Forums / Meetups / New here? / Should it be on a T-shirt? / Site Policies and FAQs / Sponsored/Guest Post Policy / Support/Donate

https://captainawkward.com

RPG Threat Models

TABLE V. I.: TREASURE IS GUARDED BY (d20)

Die	Result
1-2	Contact poison on container
3-4	Contact poison on treasure
5-6	Poisoned needles in lock
7	Poisoned needles in handles
8	Spring darts firing from front of container
9	Spring darts firing up from top of container
10	Spring darts firing up from inside bottom of container
11-12	Blade scything across inside
13	Poisonous insects or reptiles living inside container
14	Gas released by opening container
15	Trapdoor opening in front of container
16	Trapdoor opening 6′ in front of container
17	Stone block dropping in front of the container
18	Spears released from walls when container opened
19	*Explosive runes*
20	*Symbol*

THE YEAR IS 2050

"Watch your back. Shoot straight. Conserve ammo. And never, ever, cut a deal with a dragon."

—Street Proverb

Roll for initiative.

Split the party.

Touch the statue.

Attack the darkness.

A Fiendish Folio

Abuse, directed or distributed

Asymmetric costs of effort or attention

Forced participation

Security as a cost

Privacy*

*Summons 2d6 more privacy demons

…and more fiends

Asymmetric features

Unexpected design

AR and VR vectors

DevTruSafOps

Ratings without context or with irrelevant context.

Reputational damage. Reputational abuse.

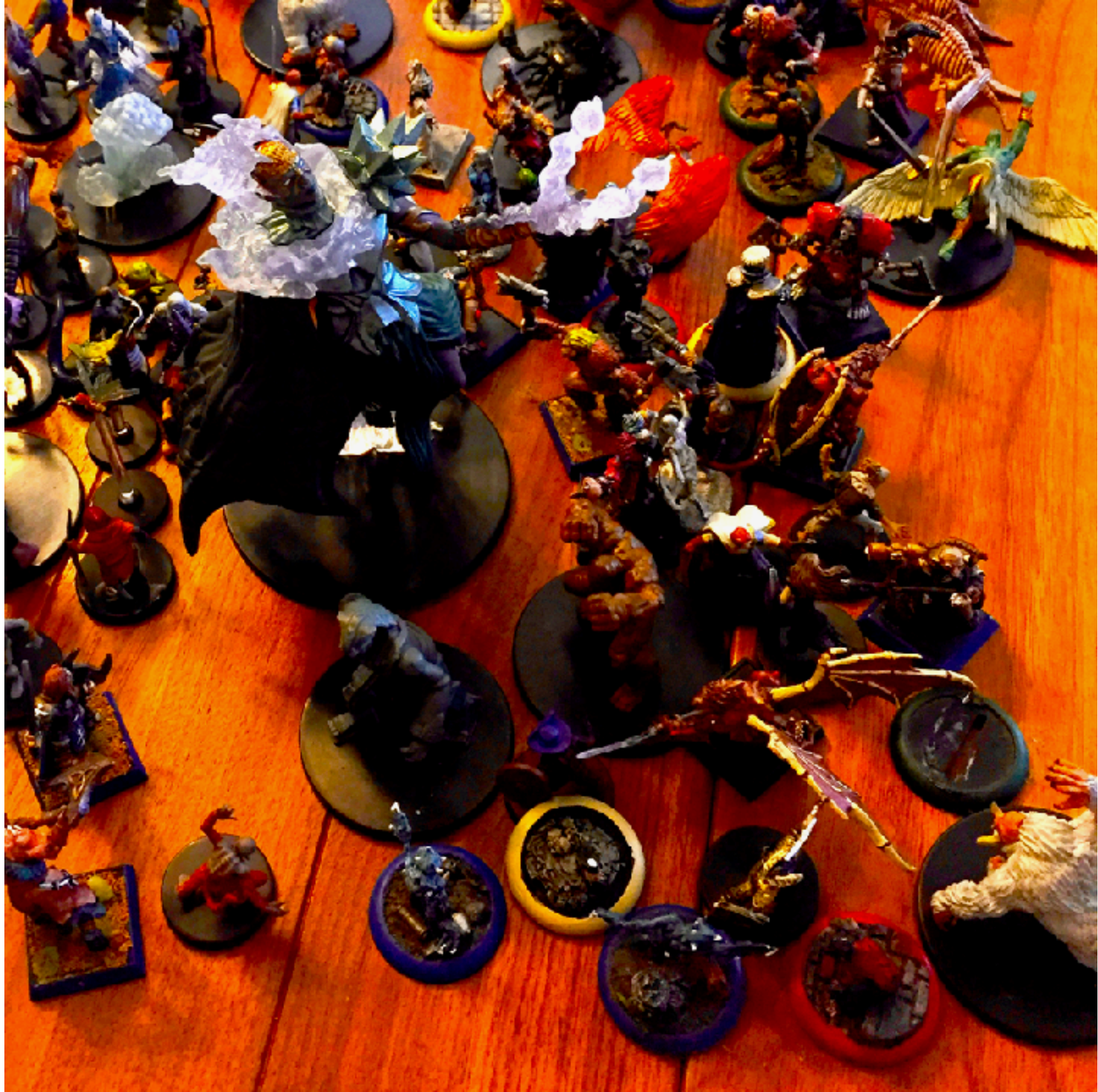
Involuntary participation, added to list of X, added to repo of Y.

DevPrivOps

Metadata leaks

De-anonymization of identity

De-aggregation of cohorts



Privacy by Design

Coarseness of data.

Storage of data.

Use of data.

CYBERDECK DESIGN TABLE

Design Formulae

Design Points = MPCP x [Hardening + ((Load Speed + I/O Speed)÷2)]

Cost = (1,000¥ x Design Points) + (Memory x 20¥) + (Storage x 20¥)

Design and Construction Time

Hardware: (Design Points÷10) x rating in days

MPCP Programming: 15 x rating in days

Other Programming: Programming size in days

Options

Response Increase:

Level 1:	+ 25 Design Points
Level 2:	+ 100 Design Points
Level 3:	+ 250 Design Points
Hitcher Jack:	+ 1 design point
Vidscreen Display:	+.5 design point

Standard Hardware is factored into the cost. It includes:

Fiber-optic connector cable terminating in an STJ-400 standard telecommunications jack.

Keyboard.

MPCP motherboard for the Persona program chips.

CLERIC SPELLS (1ST LEVEL)

CLERIC SPELLS

Protocols & Ceremonies

First Level Spells:

Ceremony (Invocation)

Level: *1*
Range: *Touch*
Duration: *Permanent*
Area of Effect: *One creature, one item, or area (see below)*
Components: *V, S, M*
Casting Time: *1 hour*
Saving Throw: *Special*

Explanation/Description: *Ceremony* has a number of applications in the religious organization, depending on the level of the cleric. The ef-

Ceremonies

How are users included in the system?

How are they modeled, what is expected of them?

Do they have the tools, knowledge, skills to accomplish what’s expected?

https://eprint.iacr.org/2007/399.pdf

Attacking the Darkness

Ambiguity in design, omitting the user.

Assuming a uniform user.

Not perceiving a user's threat model.

Not measuring a ceremony's effectiveness.


Metrics: The Observation

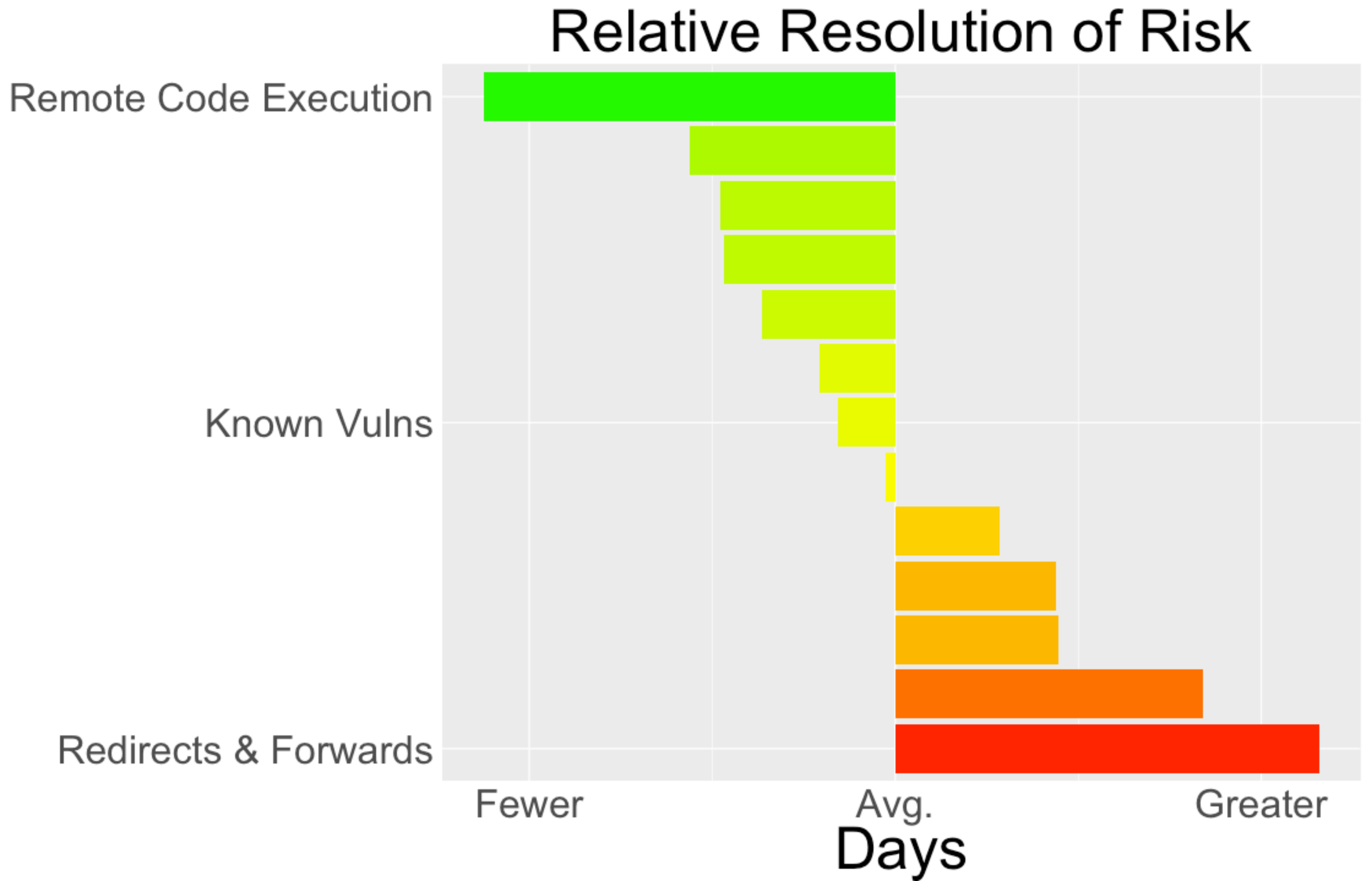
Build a Story (Cautiously)

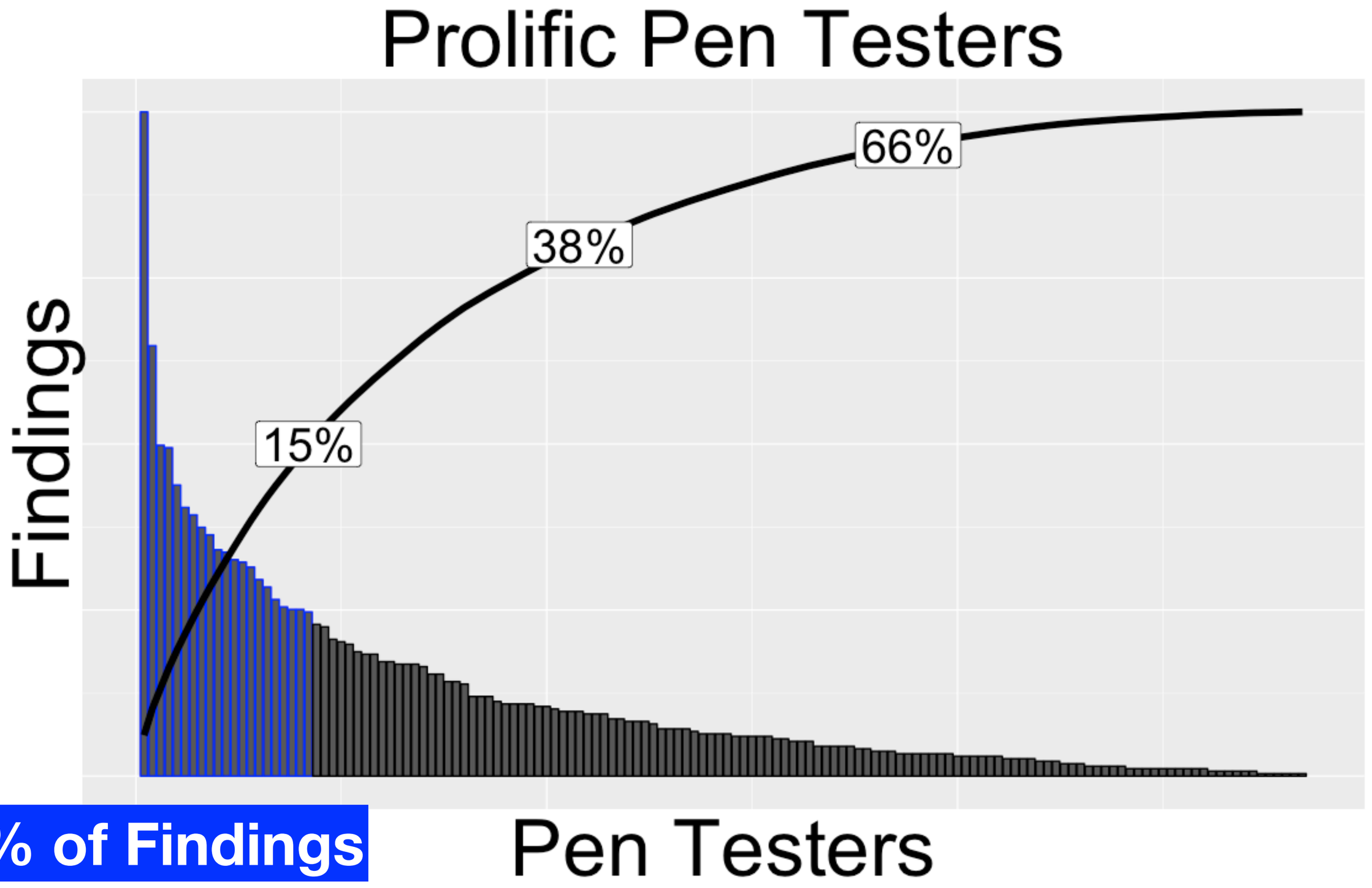
Ask an interesting & relevant question.

Collect signals, beware silence.

Create metrics, beware tunnel vision.

Create a story, beware myth.


Relative Resolution of Risk
Remote Code Execution
Known Vulns
Redirects & Forwards
Fewer
Avg.
Greater
Days


Prolific Pen Testers
Findings
15%
38%
66%
Pen Testers
50% of Findings

Threats

Lack of signals

Unrepresentative signals

Tunnel vision

Information bias & many more cognitive biases

https://www.businessinsider.com/cognitive-biases-affect-decisions-2015-8/

Unearthing Arcana

What we measure also reflects what we care about.

What we care about also reflects on our environment.

Mind Flayer

RPGs continue to evolve.

Cliques, in-groups, and gate-keeping are threats to any social group.

Not everyone is familiar with RPGs.

MIND FLAYER

FREQUENCY: *Rare*
NO. APPEARING: *1-4*
ARMOR CLASS: *5*
MOVE: *12"*
HIT DICE: *8 + 4*
% IN LAIR: *50%*
TREASURE TYPE: *B, S, T, X*
NO. OF ATTACKS: *4*
DAMAGE/ATTACK: *2 each*
SPECIAL ATTACKS: *Mind blast*
SPECIAL DEFENSES: *Nil*
MAGIC RESISTANCE: *90%*
INTELLIGENCE: *Genius*
ALIGNMENT: *Lawful evil*
SIZE: *M*
PSIONIC ABILITY: *241-340*
Attack/Defense Modes: *B/FGH*

Demogorgon, (Prince of Demons)

FREQUENCY: *Very rare*
NO. APPEARING: *1*
ARMOR CLASS: *-8*
MOVE: *15"*
HIT DICE: *200 hit points*
% IN LAIR: *50%*
TREASURE TYPE: *R, S, T, V*
NO. OF ATTACKS: *3*
DAMAGE/ATTACK: *All special*
SPECIAL ATTACKS: *See below*
SPECIAL DEFENSES: *+2 or better weapon to hit*
MAGIC RESISTANCE: *95%*
INTELLIGENCE: *Supra-genius*
ALIGNMENT: *Chaotic evil*
SIZE: *L (18' tall)*
PSIONIC ABILITY: *150/head*
Attack/Defense Modes: *All/all*

Tabletop Exercises

Scenario

Objectives

Participants

Rules & Scope

Referee

Reduces stress

Enables learning

Practices ceremonies

Generates feedback

The CTO directs a DevOps team member to improve analytics. They export a production DB into a 3rd-party business intelligence tool for a proof-of-concept.
They grant access to every team member.
The data includes password hashes.

Create relevant scenarios.

Attack the objective, not the scenario.

Review feedback on people, process, & tools.

Review feedback on rules & rulings.

RPG Interpersonal Skills

Compromise

Negotiation

Patience

Team-building

Personality (d8, d8)

1-5 Average	6-7 Extroverted	8 Introverted
1. modest	1. forceful	1. retiring
2. egoist/arrogant	2. overbearing	2. taciturn
3. friendly	3. friendly	3. friendly
4. aloof	4. blustering	4. aloof
5. hostile	5. antagonistic	5. hostile
6. well-spoken	6. rude	6. rude
7. diplomatic	7. rash	7. courteous
8. abrasive	8. diplomatic	8. solitary/secretive

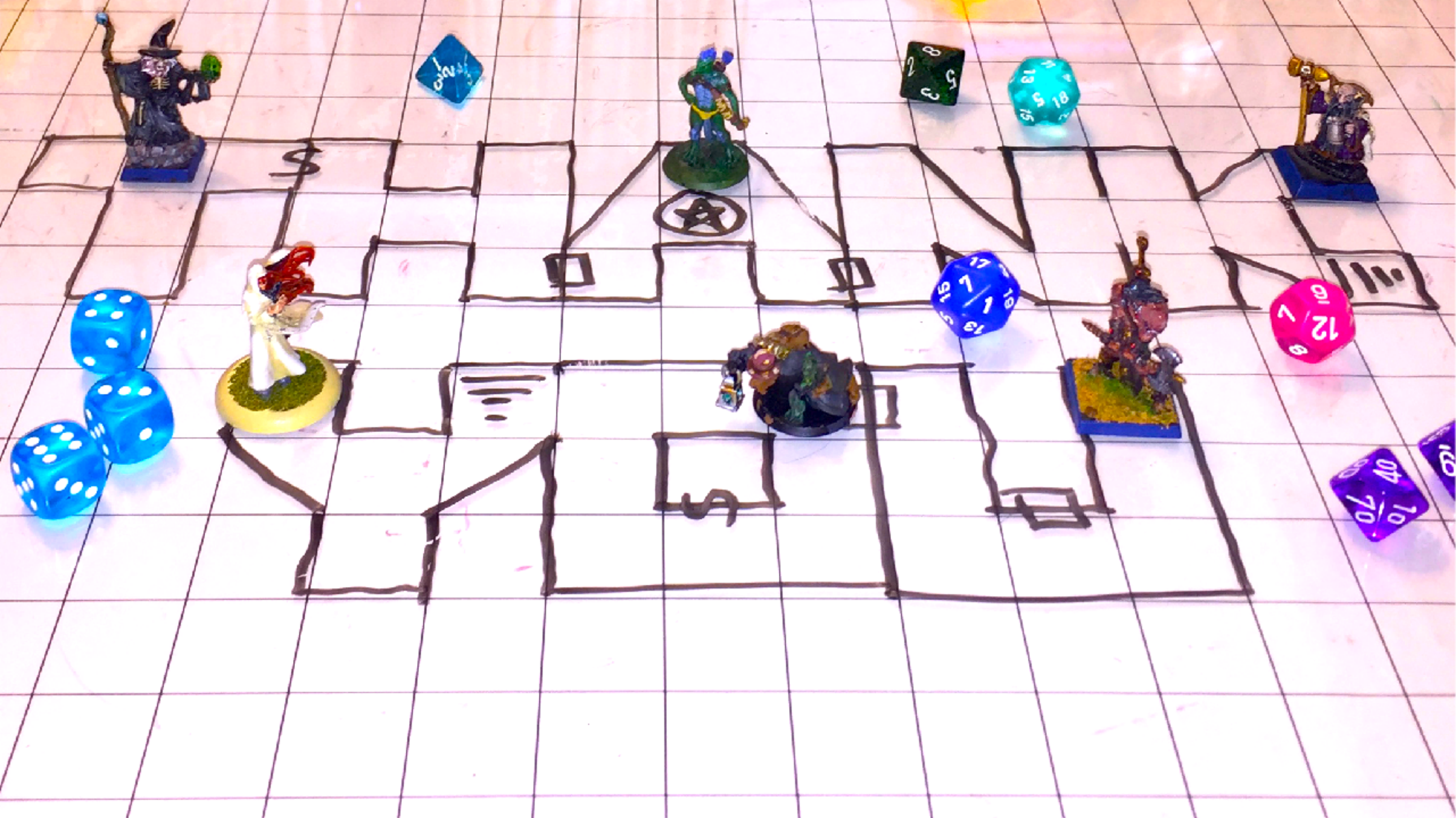
Disposition (d10)

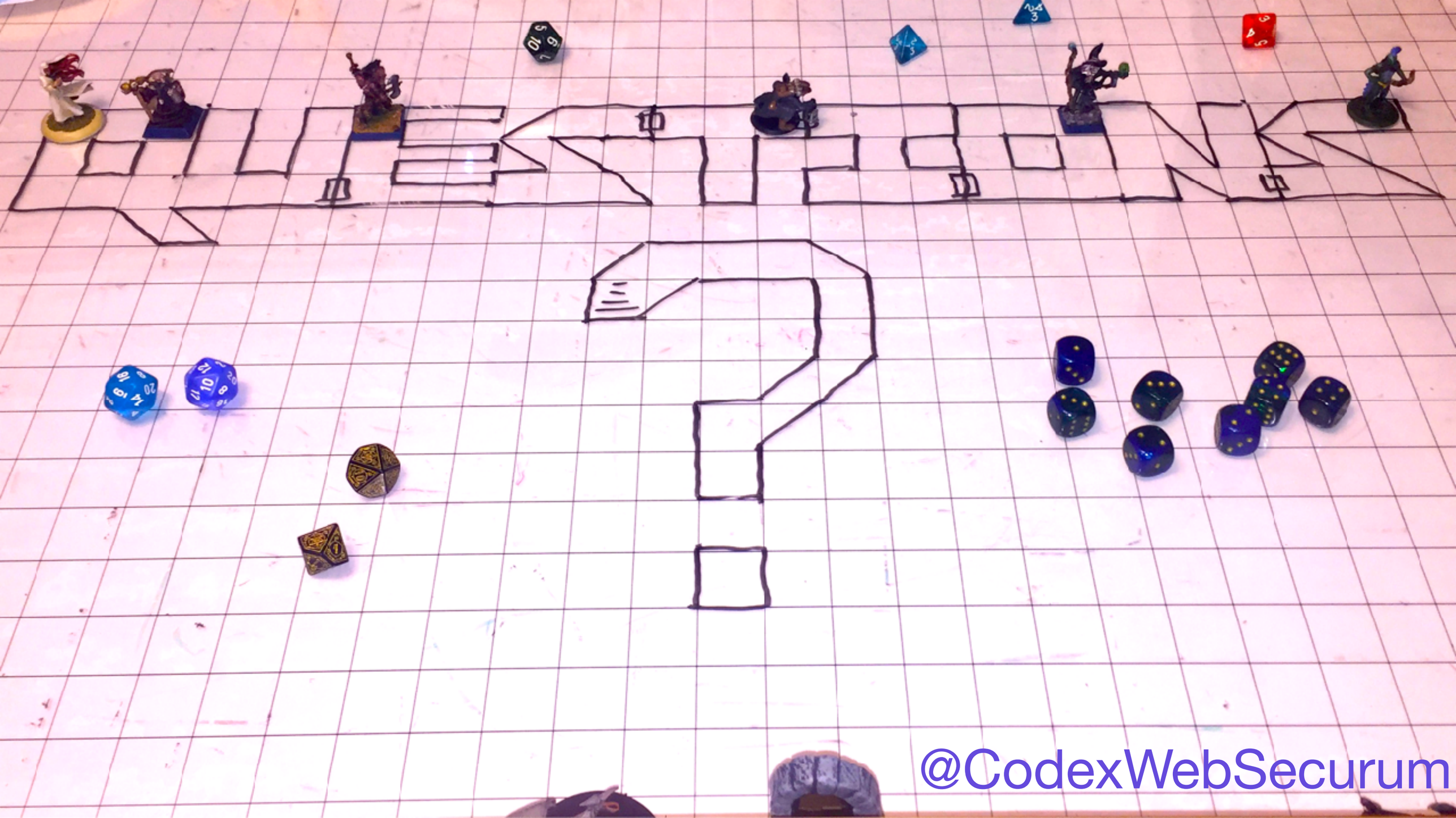
1. cheerful
2. morose
3. compassionate/sensitive
4. unfeeling/insensitive
5. humble
6. proud/haughty
7. even tempered
8. hot tempered
9. easy going
0. harsh

Made **by** people

Made **for** people

Made **of** people




@CodexWebSecurum

Appendix N

https://www.usenix.org/legacy/publications/library/proceedings/sec99/whitten.html

https://eprint.iacr.org/2007/399.pdf

https://captainawkward.com

https://www.crashoverridenetwork.com

https://geekfeminism.wikia.com/wiki/Category:Concepts

https://tallpoppy.io

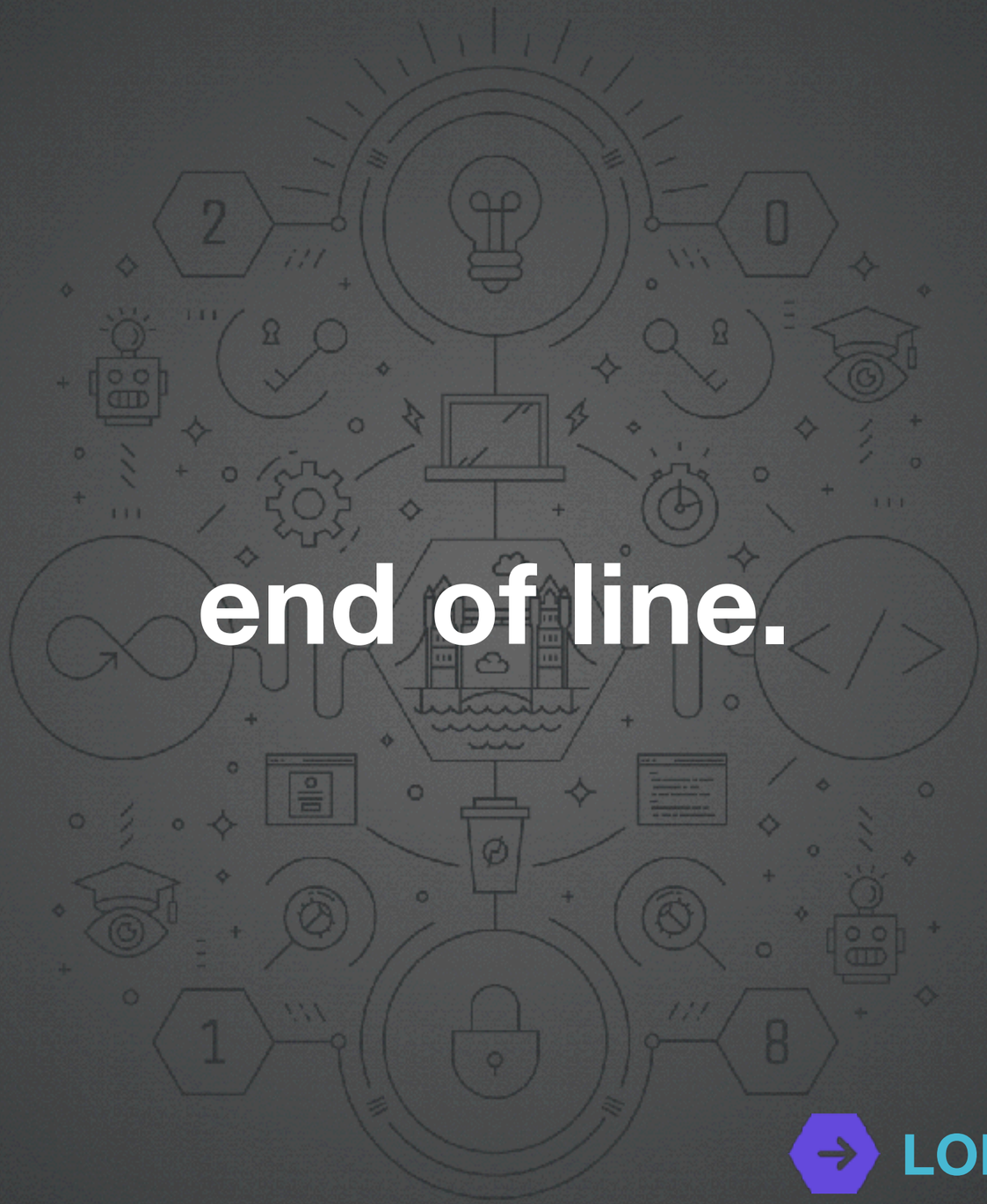
https://businessinsider.com/cognitive-biases-affect-decisions-2015-8/

https://www.contributor-covenant.org/version/1/4/code-of-conduct

“I don't wanna bust out of here and find nothing but a lot of cold circuits waiting for me.”

–*Tron,* TRON

DevSecCon



end of line.

LONDON 18-19 OCT 2018