What Game of Thrones Can Teach Us About Cyber Security

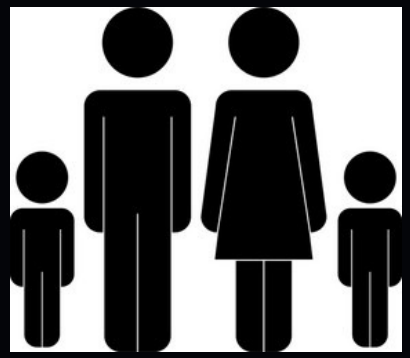
-Gerald Auger, PhD

Why this talk?

Power of storytelling

About me

SIMPLY CYBER



THE CITADEL
THE MILITARY COLLEGE OF SOUTH CAROLINA

Simplycyber.io/socials

SPOILERS AHEAD

Winterfell
White Harbor
Port of Ibben
Ib Sar
New Ibbish
Braavos
Lorath
Morosh
Saath
The Eyrie
Gulltown
Riverrun
Pyke
Casterly Rock
Lannisport
King's Landing
Norvos
Pentos
Qohor
Kingdom of the Ifequevron
Vaes Dothrak
Kayakayanaya
Nefer
Mossovy
The Thousand Islands
Plains of the Jogos Nhai
Dothraki Sea
Highgarden
Tyrosh
Myr
Samyrian
Trader Town
K'Dath
Bonetown
Meereen
Hesh
Kosrak
Yunkai
Lhazosh
Mantarys
Ely
Tolos
Tiqui
Oldtown
Sunspear
Lys
Volantis
Astapor
Bayasabhad
City of the Wing Men
Westeros
Essos
Qarth
Asabhad
Yi Ti
Jinqi
Leng Yi
New Ghis
Faros
Yin
Vahar
Leng Ma
Turrani
Lotus Point
Summer Sea
Sunset Sea
Summer Islands
Port Moraq
Zabhad
Asshai
Sothoryos
Jade Sea
Ebonhead
Ulthos

Dimensions to Apply Learning

- roles
- Processes
- Capabilities
- Case study
- career

Let’s meet our players

Ned STark

- High integrity
- Leadership
- Vigilance and preparedness

Winter is coming

CISO

- High integrity
- Leadership
- Vigilance and preparedness

threats
Are
coming

CISO

- Accountable
- Moral decisions
- Allies turned on him

Political intrigue

Cersei lannister

- Ambitious
- Political mastermind
- Budget Power plays

Business leaders

- Power dynamics
- Sabotaging agendas
- Power of partnerships

Small council

- serves as advisors to the King of Westeros
- responsible for making key decisions

The board

- diverse backgrounds
- allocate financial resources
- overseeing risk management

- Speak their language

White walkers

- Origins shrouded in mystery
- Recruitment and expansion
- Deliberate and focused attacks

Threat actors

- Unknown origins and ideology
- Botnets , weaponized tooling, insiders
- Actions on objective – persistence and exfil

Shout out to tyrion

- Low to no budget infosec pro
- Savvy and scrappy to resolve issues
- Leverages resources available

Capabilities to play the game

The sparrows

- Religious sect
- a means to an end
- Faith militant
- Cersei full compromise

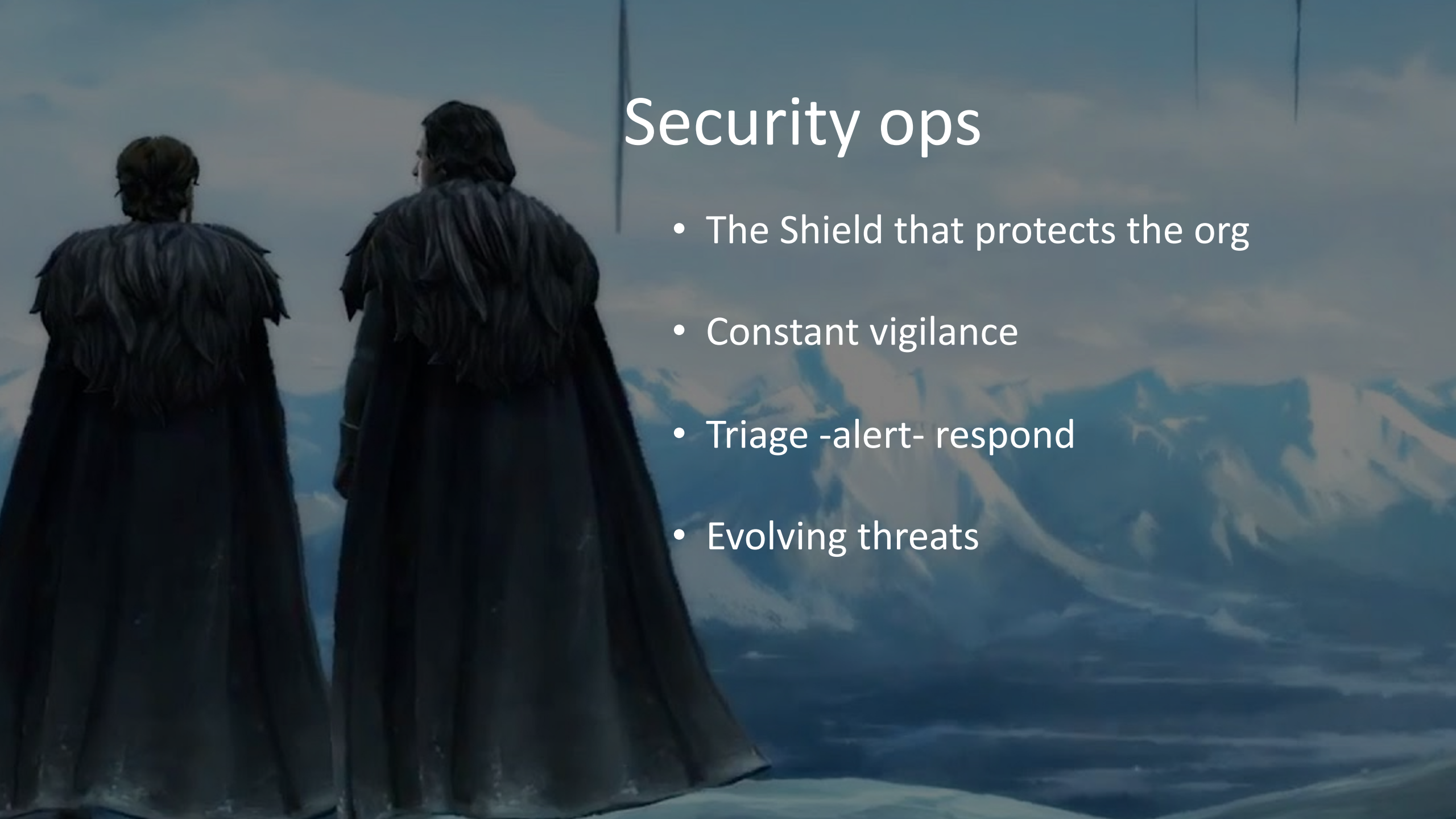
Risk analysis

- Yassss grc!
- Underestimated threat
- Misunderstood motivations
- Over permissioned access
- Massive cost to correct

SHAME. SHAME. SHAME.

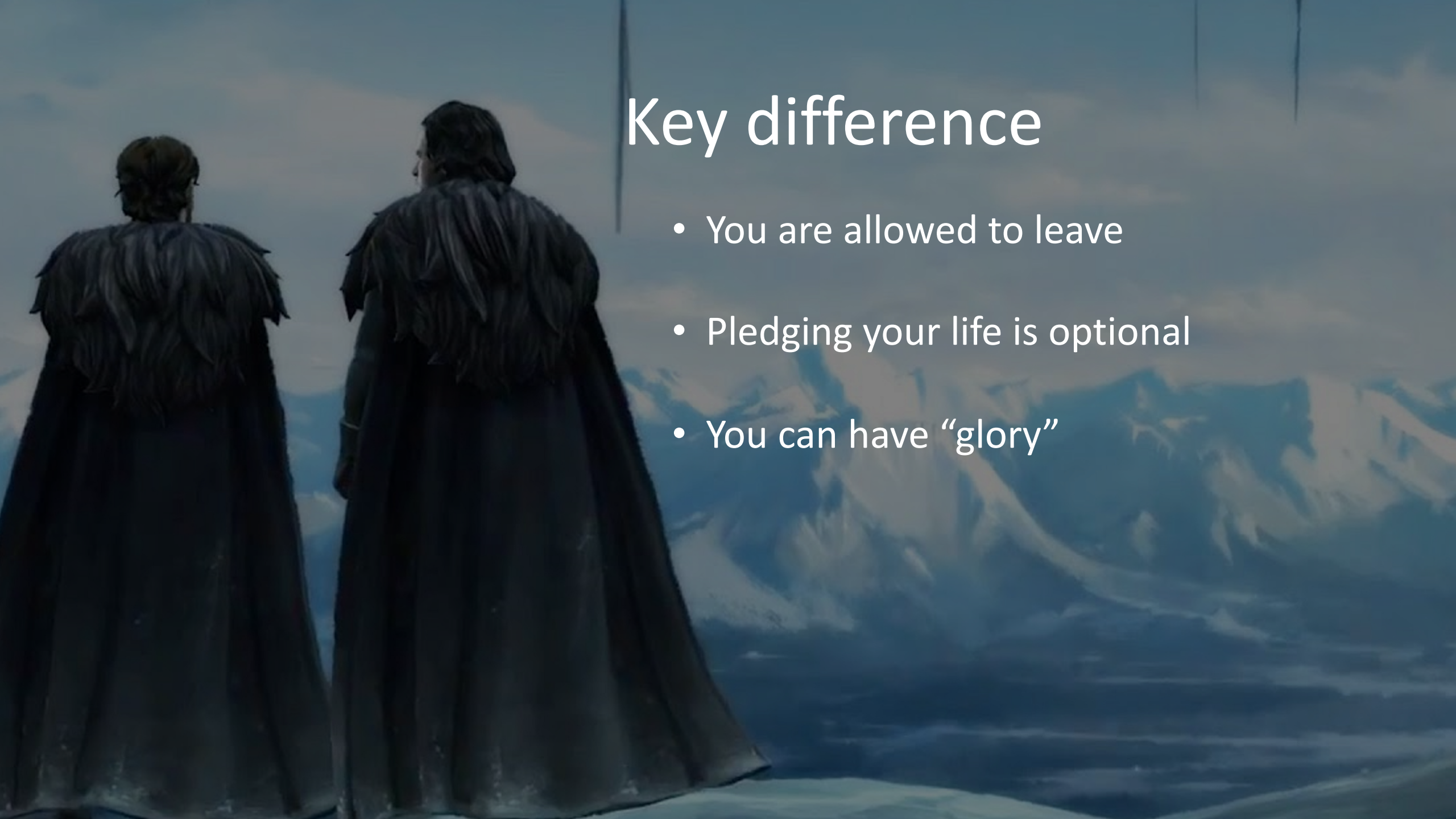
Night’s watch

- I am the watcher on the walls
- the horn that wakes the sleepers
- the shield that guards the realms of men



Security ops

- The Shield that protects the org
- Constant vigilance
- Triage -alert- respond
- Evolving threats



Key difference

- You are allowed to leave
- Pledging your life is optional
- You can have “glory”

viserion

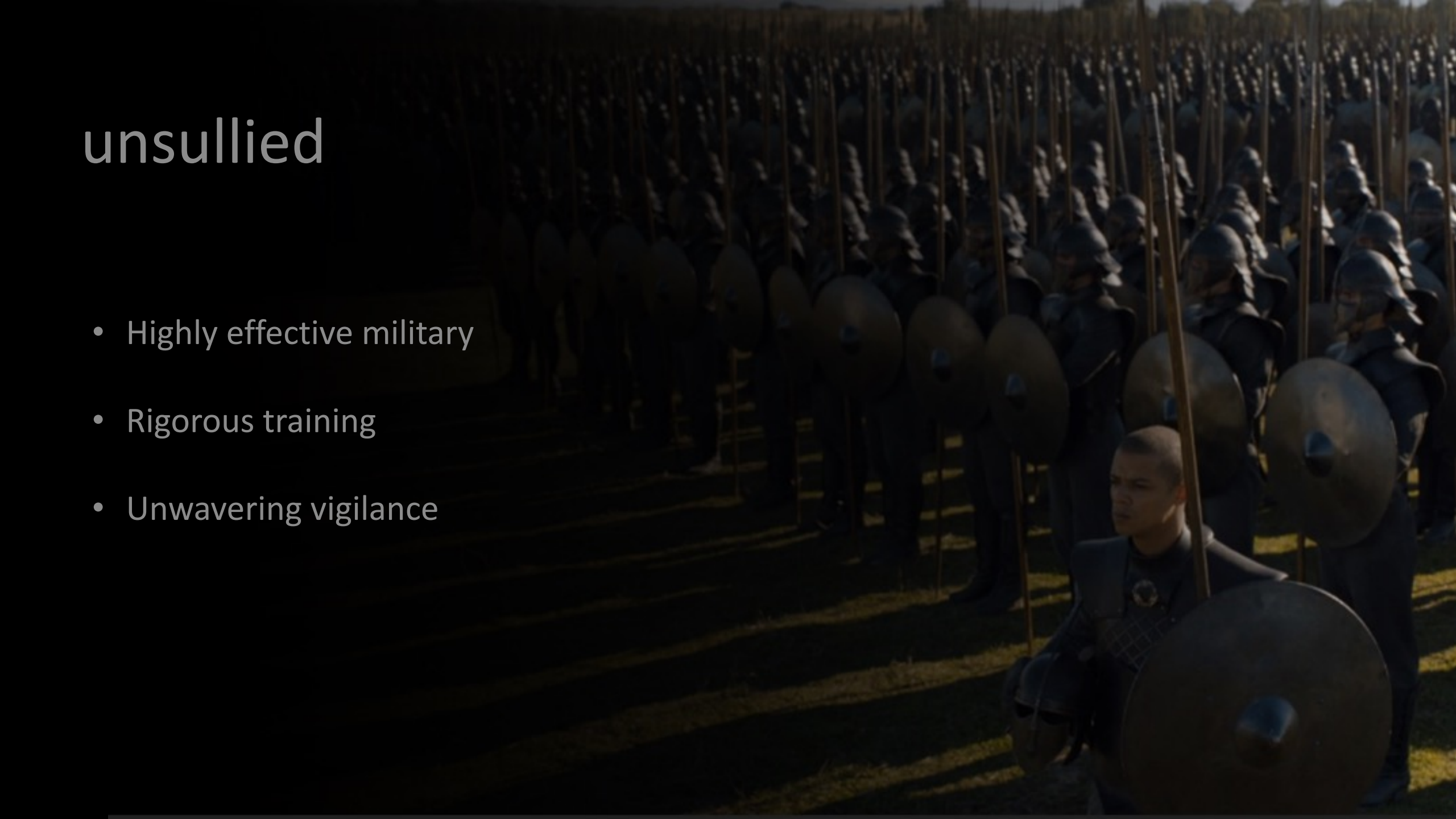
- A powerful dragon
- Advantageous Weapons system
- Converted by night king to an ice dragon

Weaponized tooling

- Powershell
- Cobalt strike
- Lolbas-project. github.io

unsullied

- Highly effective military
- Rigorous training
- Unwavering vigilance



Consistent training

- Tabletop exercises
- End user awareness
- Focused security training

Varys
Master of whispers

- known for extensive spy network
- gathers Intel from various sources
- keep those in power informed

Threat intel

- Data collection - Little birds – Telemetry
- Analysis - intention and motivations
- Actionable - Serve the “realm”

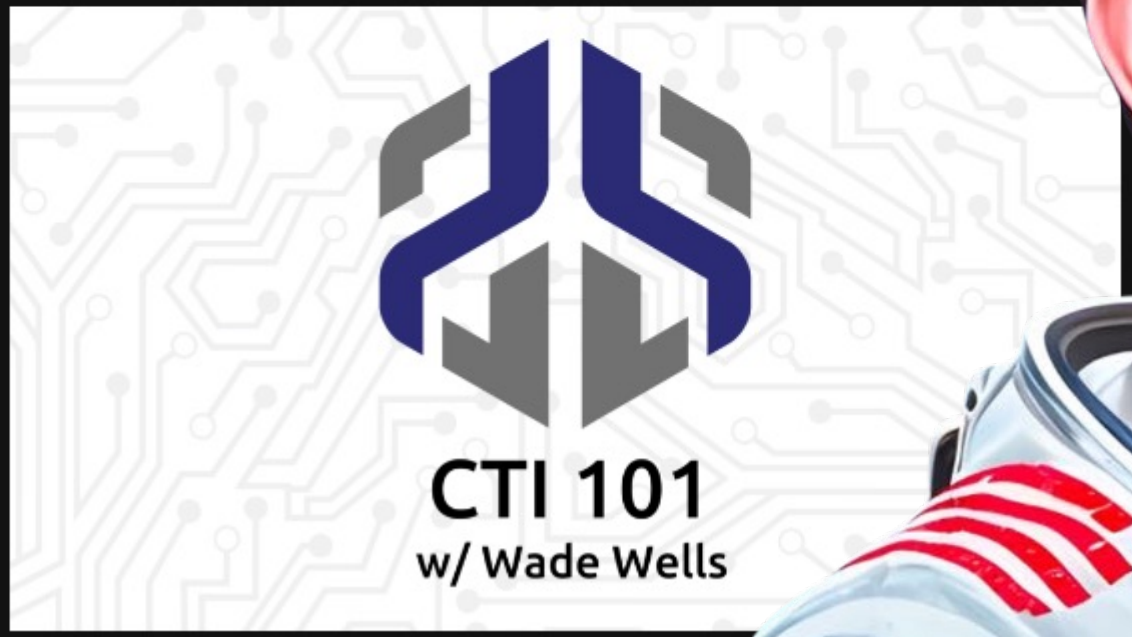
Cyber Threat Intelligence 101 w/ Wade Wells

June 20 @ 9:00 am – 6:00 pm EDT

Instructor: Wade Wells

Course Length: 8 Hours

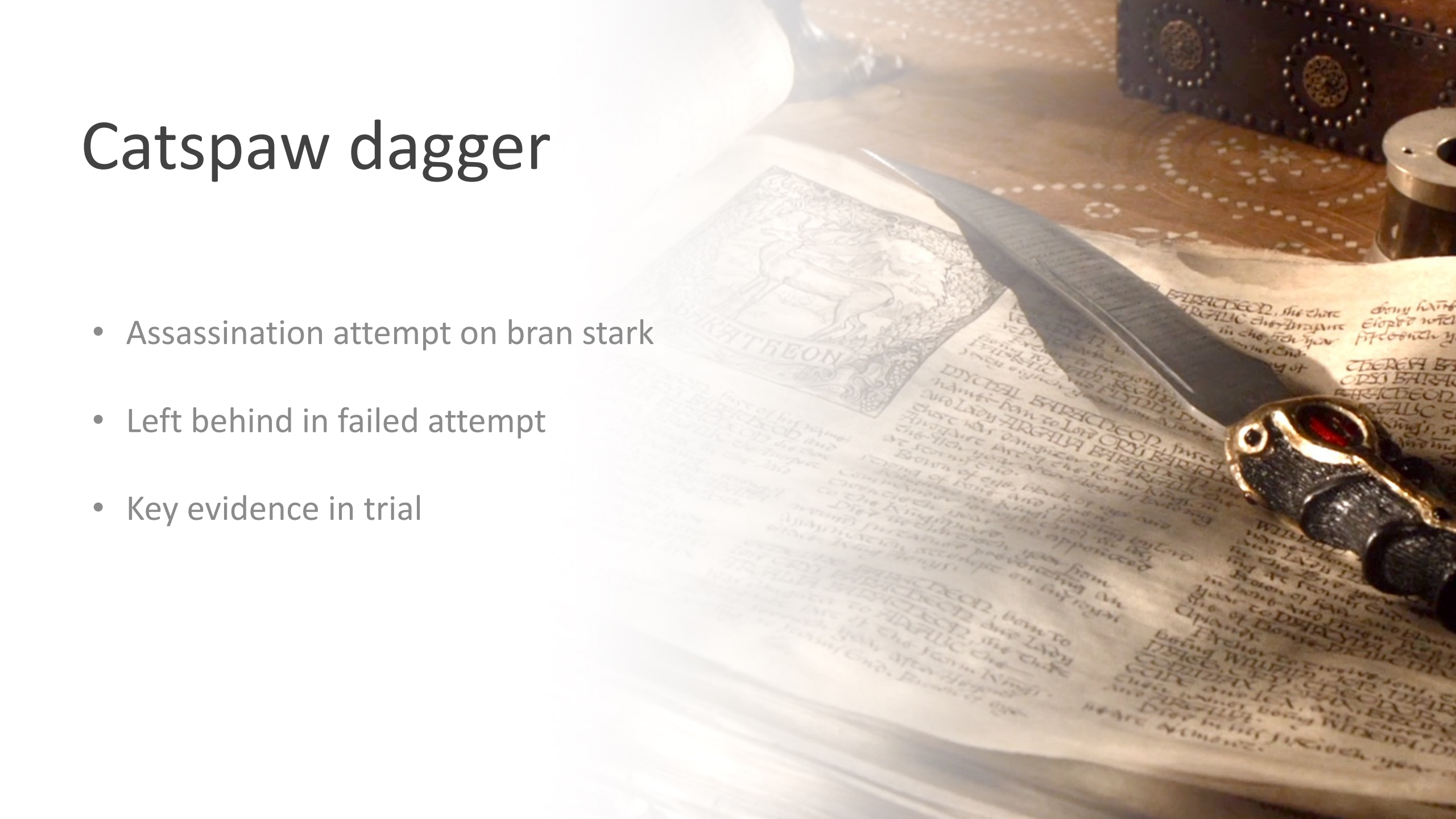
Includes: Six months of complimentary access to the Antisyphon Cyber Range, certificate of participation, six months access to class recordings.



the Processes to execute

Catspaw dagger

- Assassination attempt on bran stark
- Left behind in failed attempt
- Key evidence in trial



Security breach

- Attack - detect - ir
- Misattribution
- Failed root causes analysis

Sam and Oldetown

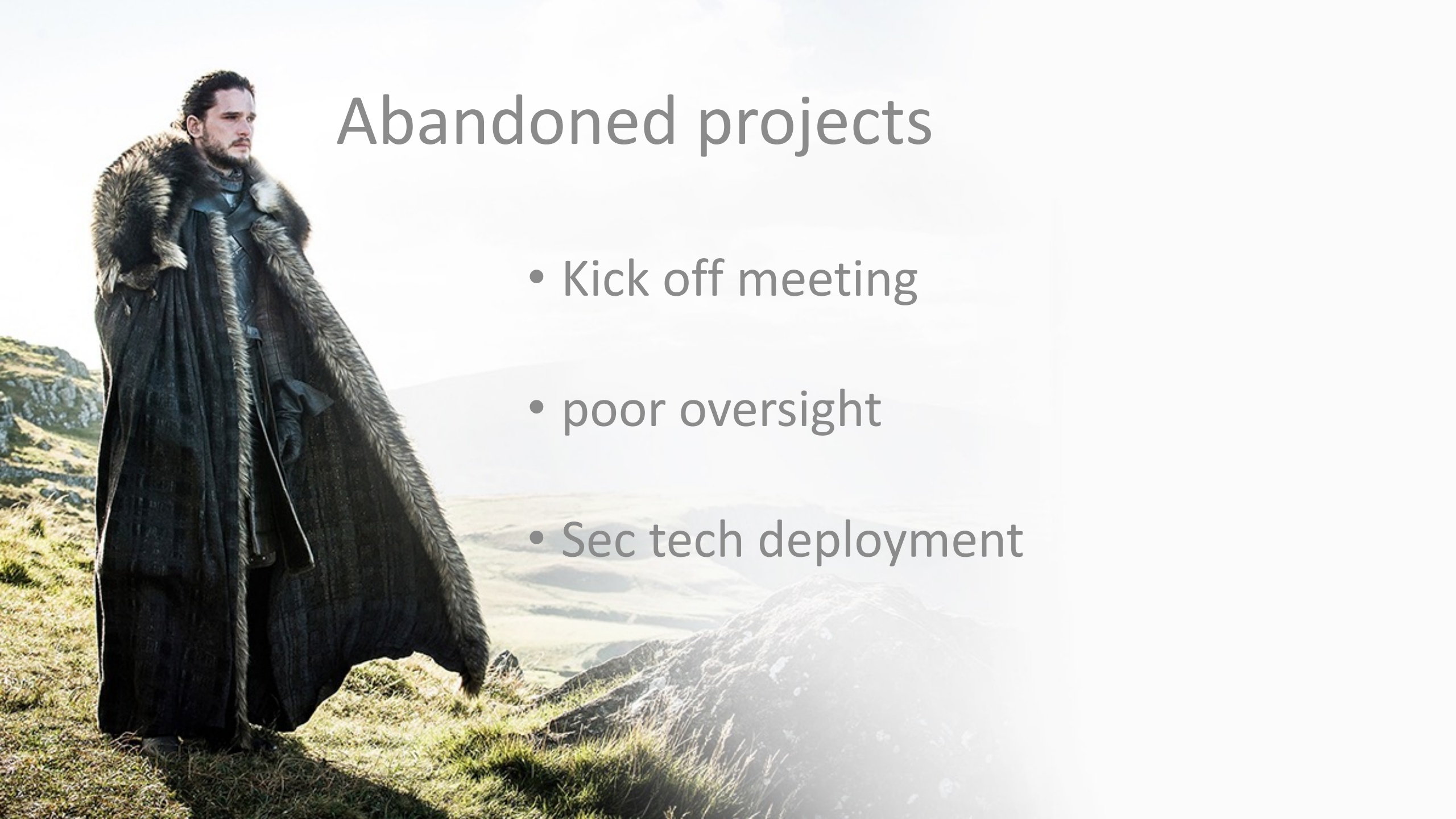
- Documented known knowledge
- Dragonglass cache
- Greyscale treatment

documentation

(Hold your boos for the end)

- Tactical: Iocs, isacs
- Operational: Sops, wiki , lessons learned
- Process improvement

Jon
Snow targaryen whatever



Abandoned projects

- Kick off meeting
- poor oversight
- Sec tech deployment

Sept of baelor

- Church major power player
- destroyed all “threats” inside
- Catastrophic failure

How not to do disaster recovery

- All material assets collocated
- Lack of risk assessment
- Zero contingency

the cyber career
is dark and full of terrors

Sansa

- Naïve to battle hardened
- experiences that shaped her
- Queen of north

Sansa

- Day 1 and
  Day 90 in infosec
- Lessons learned to predict future threats
- case study

The Hound And sansa

- Hostile
- Shared experiences
- Complex morality

Give Mentorship

- Protect and guide
- Not typical mentor
- Build confidence

Sansa and olenna tyrell

- Empowerment and honesty
- Mutual respect
- Shared desire to challenge status quo

Take Mentorship

- Be receptive
- Mutual respect
- Mentorship in many forms

Cersei
And sansa

- Manipulation and deceit
- Power dynamics
- False security

Avoid toxicity

- Mentor and mentee dynamic
- Work ORG structure
- Malicious community

You know nothing jon snow

- sheltered life vs realities
- Professional growth path

You know Something jon snow

- Hands on skills
- Value of education
- No easy button but ample opportunity

Jamie lannister

- Loses primary hand in battle

- Continue to Deliver value
  - Battle strategist
  - King counsel
  - diplomacy

Professional development

- You can pivot w/in cyber
- Find your passion
- Identify economies of scale

998th Lord Commander

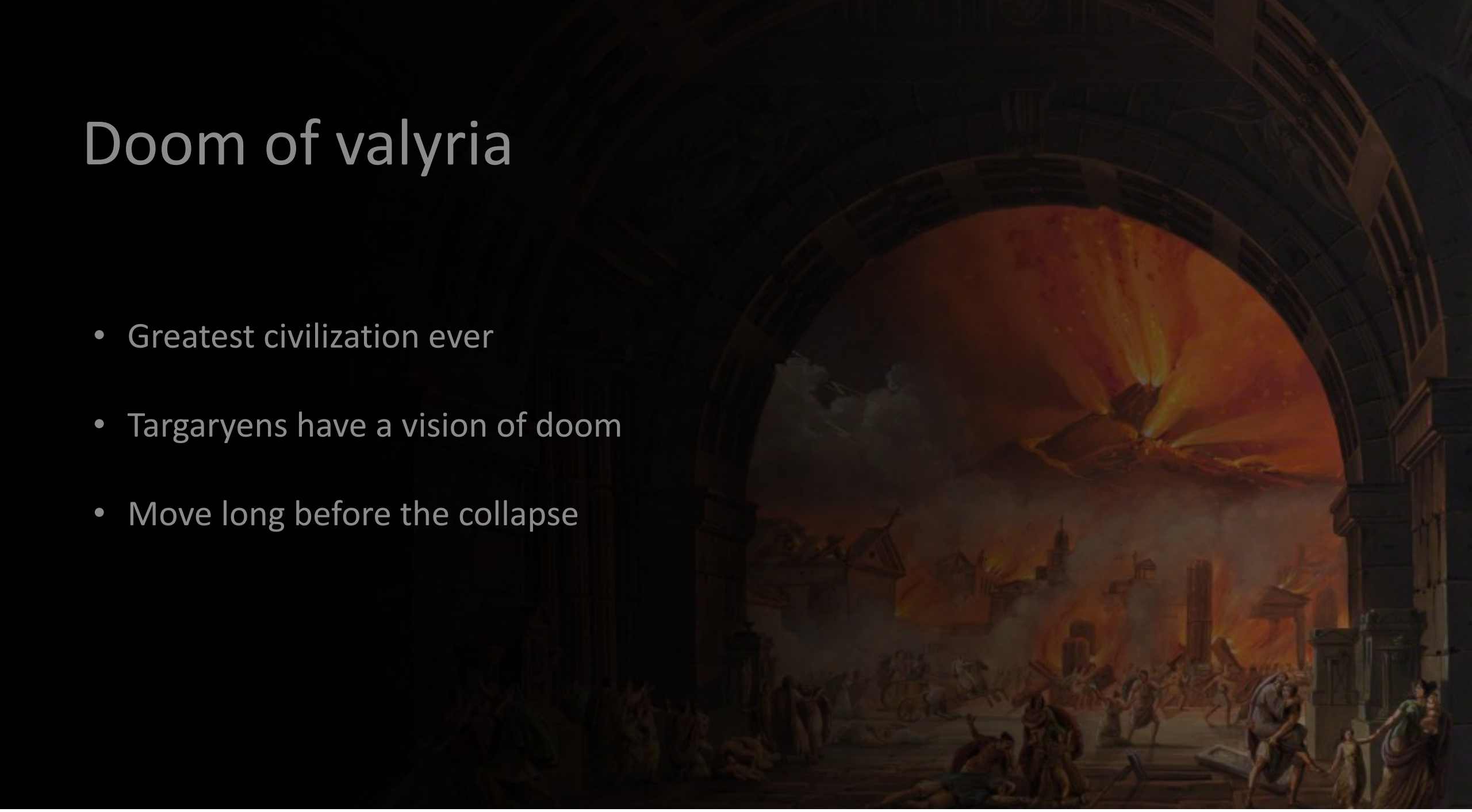
- Fierce competition
- Warriors, stewards, builders
- Elected jon snow by nights watch

NETWORKING

- Empathetic with all factions
- Delivered on commitments
- Saw value and engaged in others

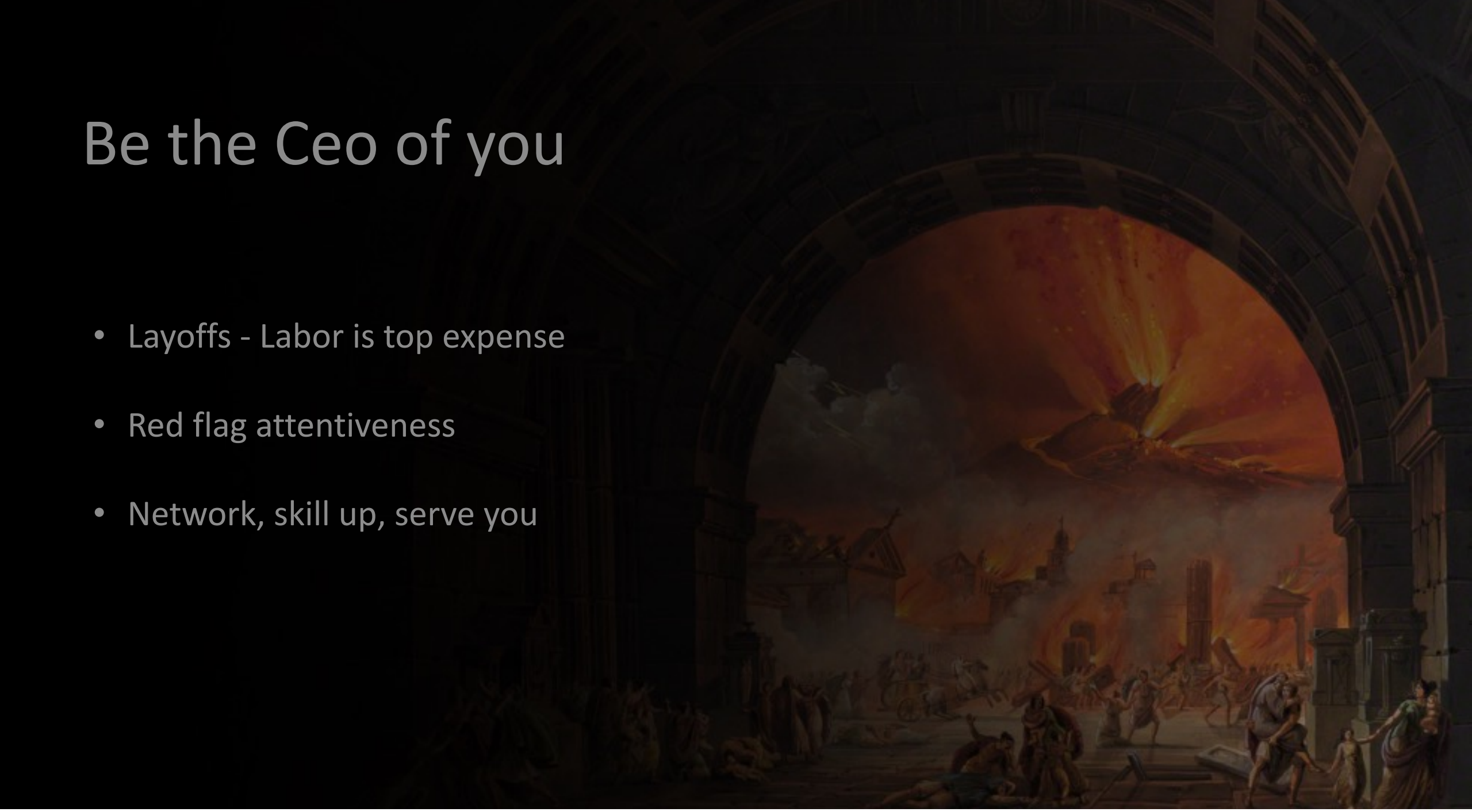
Doom of valyria

- Greatest civilization ever
- Targaryens have a vision of doom
- Move long before the collapse



Be the Ceo of you

- Layoffs - Labor is top expense
- Red flag attentiveness
- Network, skill up, serve you



Story unfinished

- Last book released in 2011

Your Story unfinished

- Find your passion
- Infinite educational stimulation
- Find a focus and lean into it

Connect with me

Gerald auger, Phd

Simplycyber.io/socials