Realigning From Chaotic Evil

@JoeSchottman

About Me

Security R&D at Truist, Geek

Application Security, Pen Testing, Blue Team, Purple Team, Incident Response, DevOps, Operations, Web Developer, Sysadmin

Enterprisey

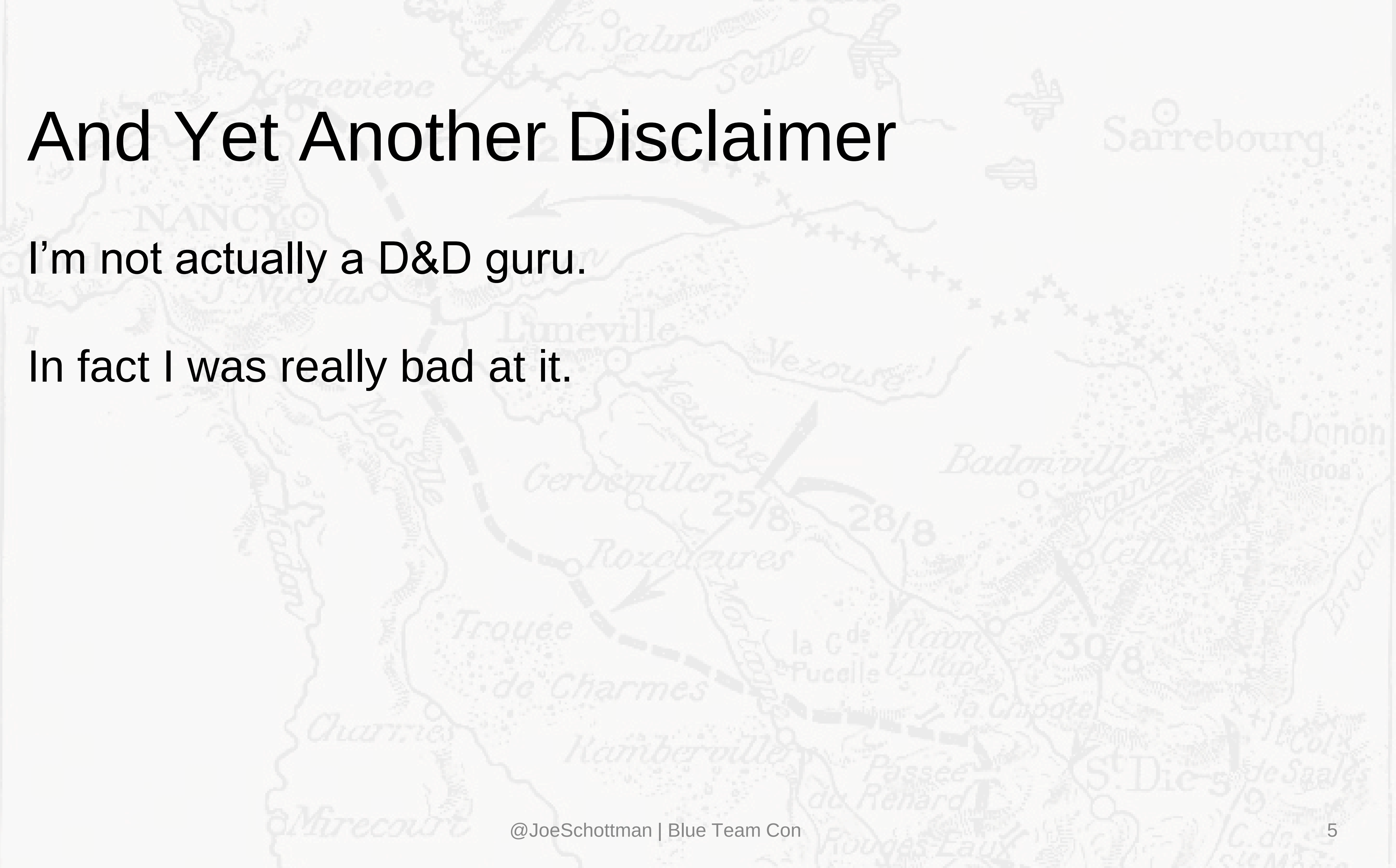
Obligatory Disclaimer

Not speaking on behalf of Truist or any other entity. All opinions expressed are my own.

All images are believed to be public domain, Creative Commons, used with permission, or created for the presentation.

Additional Disclaimer

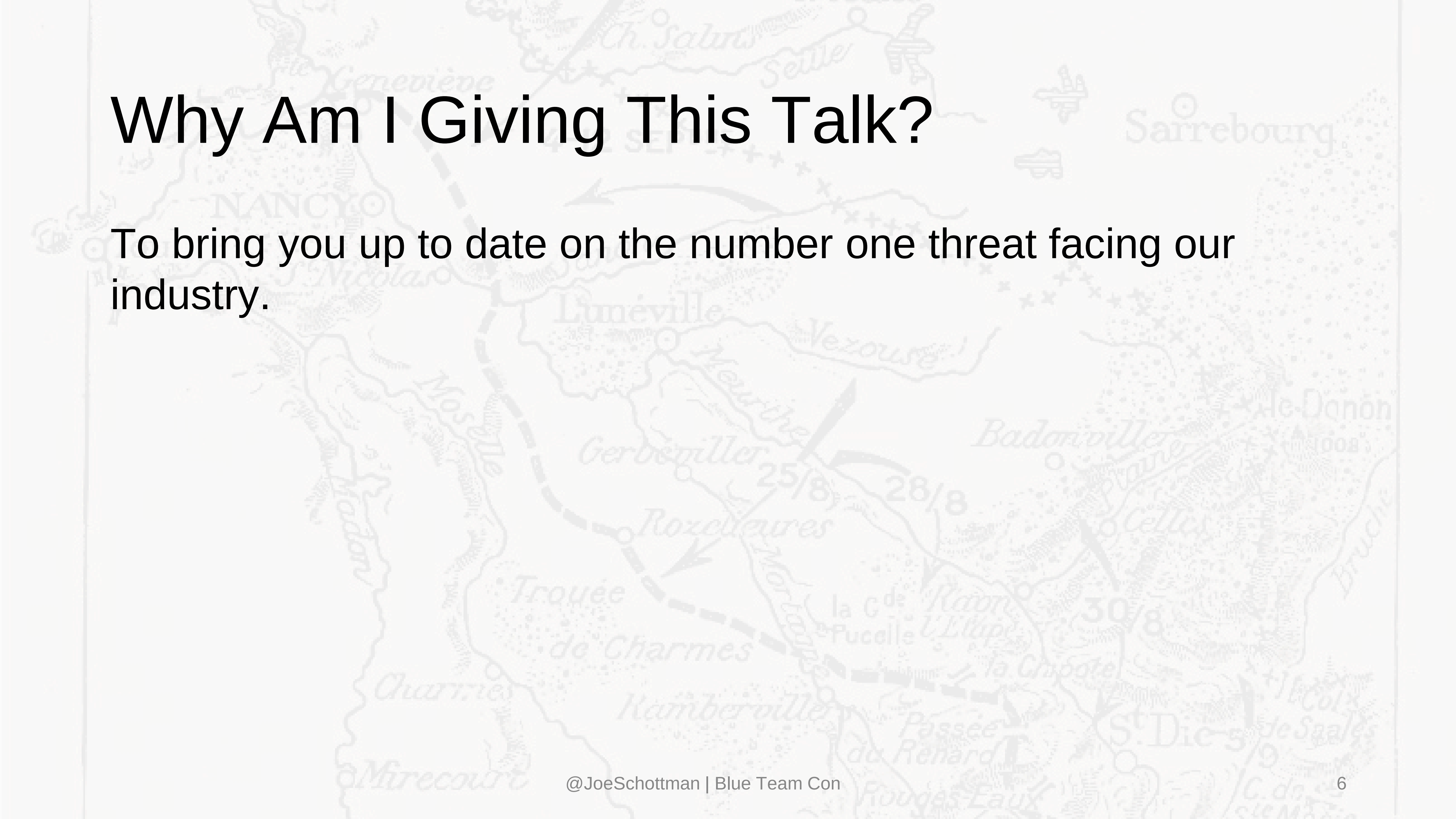
I’m not just talking about my employers.



And Yet Another Disclaimer

I’m not actually a D&D guru.

In fact I was really bad at it.



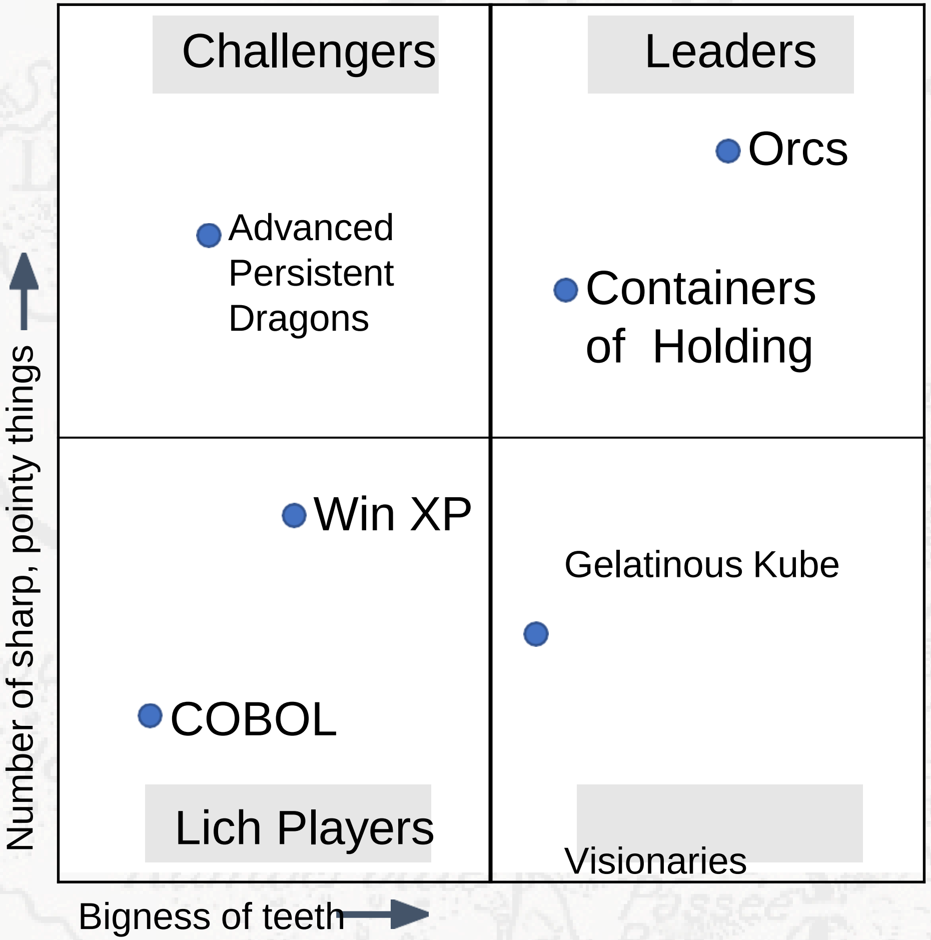
Why Am I Giving This Talk?

To bring you up to date on the number one threat facing our industry.

Orcs.

Gandalf Magic Quadrant

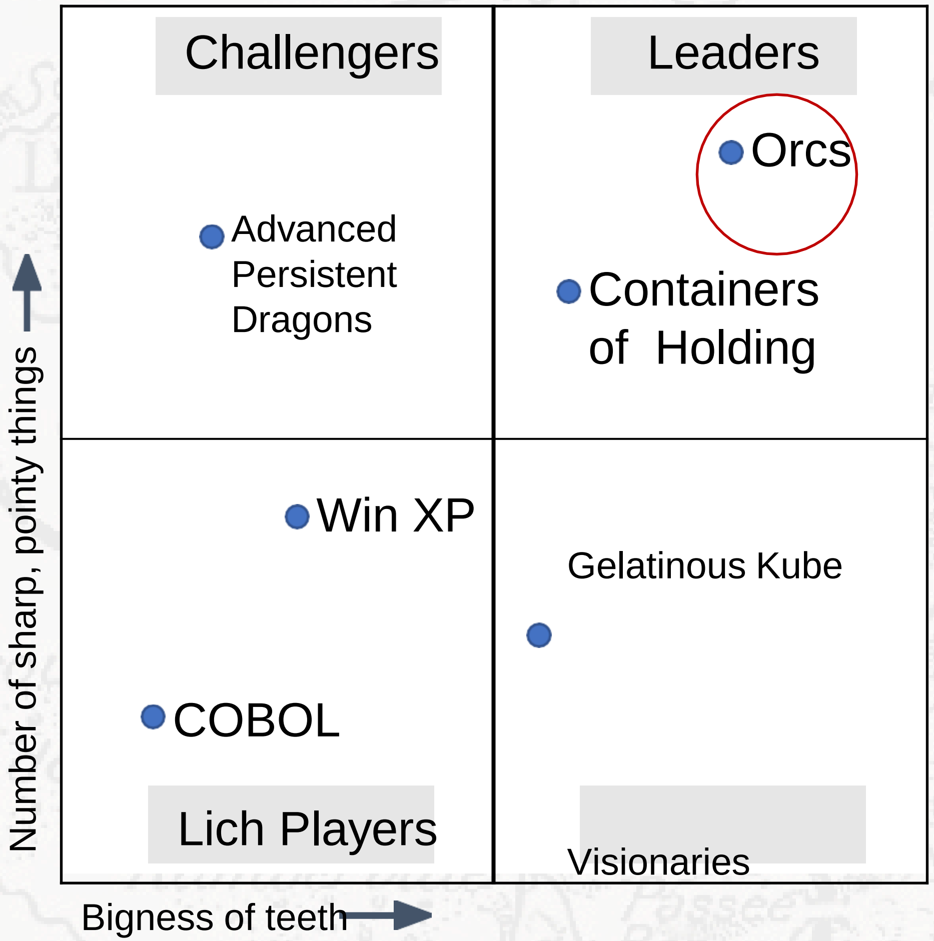
Cyber Threats 2021



©Gandalf

Gandalf Magic Quadrant

Cyber Threats 2021



©Gandalf

No, Seriously, Why Am I Giving This Talk?

REALIGNING CORPORATE SECURITY OBJECTIVESTO SYNERGIZE EFFICIENCIES

SOCIAL ENGINEERING YOUR WAY TO SECURITY SUCCESS

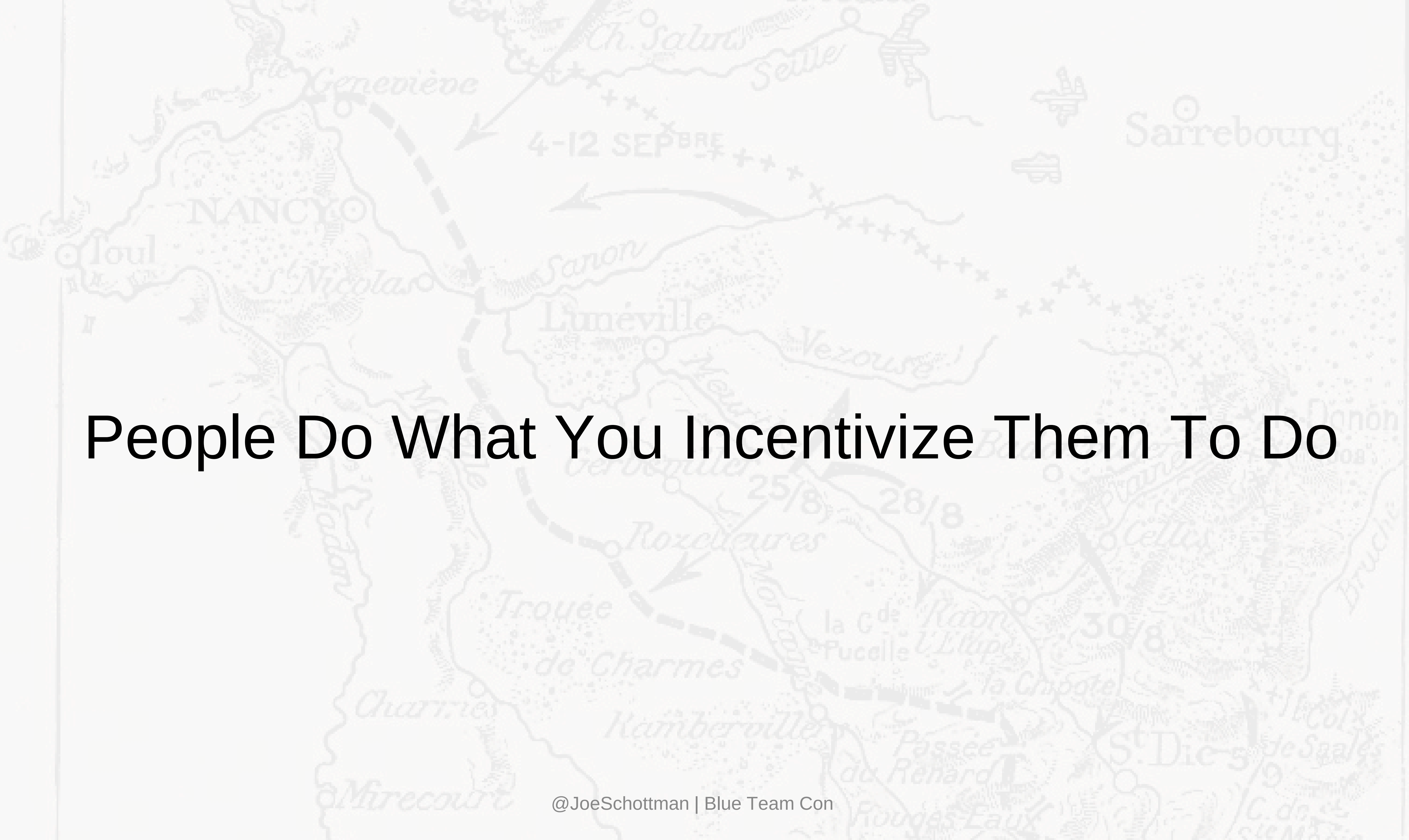
No, Seriously, Why Am I Giving This Talk?

Corporations often don’t align incentives with increasing security.

Let’s try to fix that.

The Bard’s Tale

If someone only works on projects that management rewards progress on,
are they a jerk?



People Do What You Incentivize Them To Do

What Is (A)D&D?

A fantasy role playing game where players take on the persona of mythical characters to tell a collaborative story with the help of dice.

Inspired by Tolkien's Lord Of The Rings mythos.

What Is Alignment?

Good implies altruism, respect for life, and a concern for the dignity of sentient beings. Good characters make personal sacrifices to help others.

Evil implies harming, oppressing, and killing others. Some evil creatures simply have no compassion for others and kill without qualms if doing so is convenient or if it can be set up. Others actively pursue evil, killing for sport or out of duty to some malevolent deity or master.

What Is Alignment?

Law implies honor, trustworthiness, obedience to authority, and reliability. On the downside, lawfulness can include closed-mindedness, reactionary adherence to tradition, judgmentalness, and a lack of adaptability.

Chaos implies freedom, adaptability, and flexibility. On the downside, chaos can include recklessness, resentment toward legitimate authority, arbitrary actions, and irresponsibility.

Balanced Groups Have Similar Alignments

Don’t Mix These Characters

Marco Hazard

Lego Fantasy Scenary - Knight's Resting Ver

2.0 https://creativecommons.org/licenses/by-sa/2.0/

https://www.flickr.com/photos/42405591@N02/1162 2384283/in/photostream/

With These

Marco Hazard

Lego Stuff - Necromancer Army Updated

https://creativecommons.org/licenses/by-sa/2.0/

https://www.flickr.com/photos/42405591@N02/1709 1633788

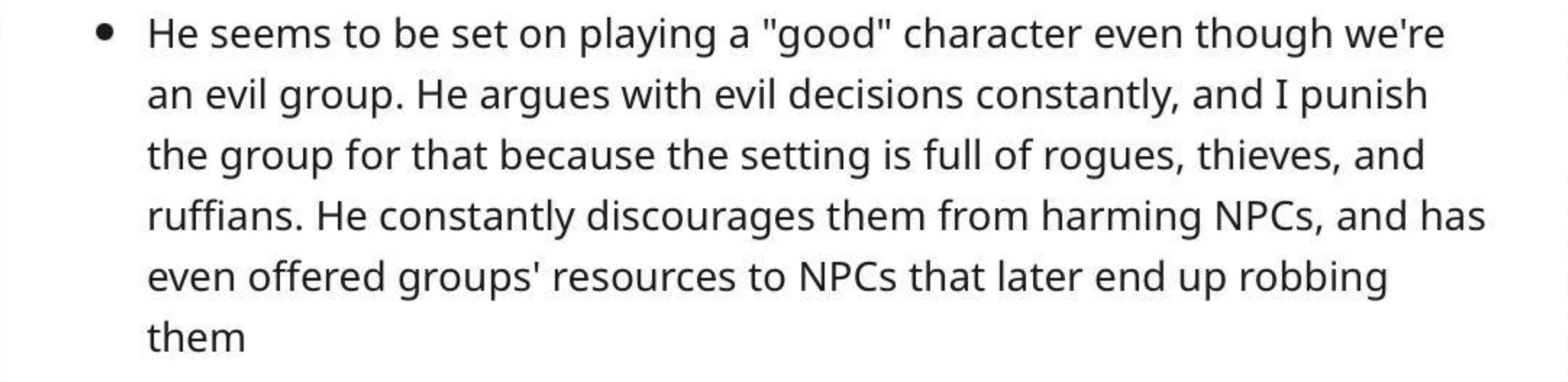
Or You Get This

Marco Hazard

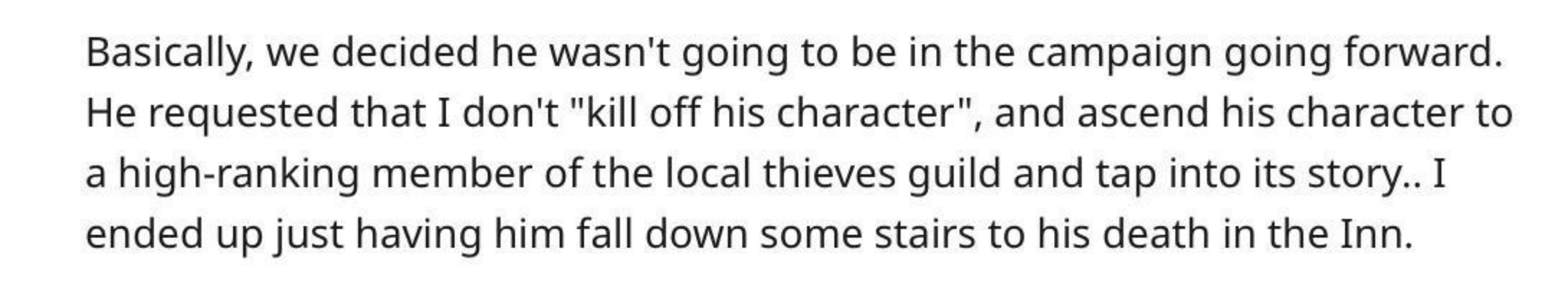
Lego Fantasy Scenary - They Can't Co-exist

https://creativecommons.org/licenses/by-sa/2.0/

https://www.flickr.com/photos/42405591@N02/1162 2515344/



- He seems to be set on playing a "good" character even though we're an evil group. He argues with evil decisions constantly, and I punish the group for that because the setting is full of rogues, thieves, and ruffians. He constantly discourages them from harming NPCs, and has even offered groups' resources to NPCs that later end up robbing them



Basically, we decided he wasn't going to be in the campaign going forward. He requested that I don't "kill off his character", and ascend his character to a high-ranking member of the local thieves guild and tap into its story.. I ended up just having him fall down some stairs to his death in the Inn.

Offensive Security As Evil

Common Red Team Incentives

Objective based

- Get shell/root/domain admin
- Generate scary reports
- Able to exfil 3 million credit card numbers after reading the CEO’s private e-mail
- Do n number of tests/quarter

At the end of the day, offensive security can’t reduce risk in and of itself.

Defensive Security As Good

Blue Team

- SOC Analysts
- Threat Intel
- Forensics/Malware Analysts

The Blue Team Is Sometimes Restrained

Common SOC complaints

- Long shifts
- Lack of training
- Lack of advancement
- Lack of opportunity to learn and experiment
- Lack of funding

Differently Aligned

May fall under different management that the Red Team, with very different metrics and incentives.

Some common Blue Team Metrics:

- Number of tickets closed
- Reaction time to alerts
- Play/run books created
- Not appearing in newspapers as having been owned

Conflict

The Blue Team sees the Red Team as a force of chaotic evil.

The Red Team sees the Blue Team as being too tied down to lawful order.

Developers

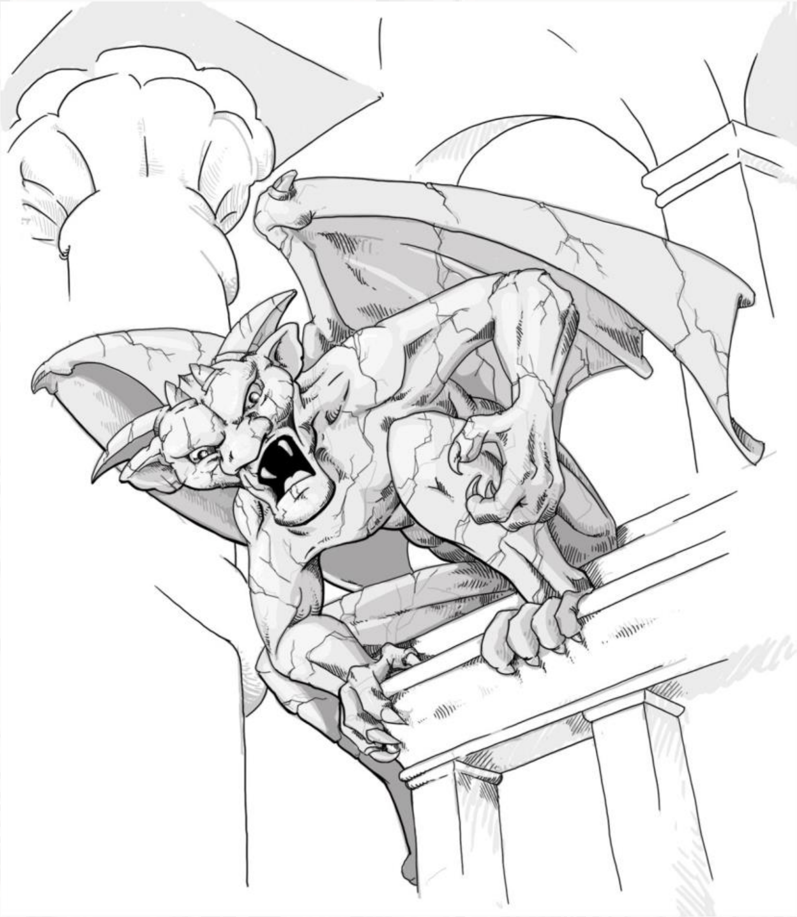
Often incentivized by new features rather than stability or security.

Operations

Often incentivized by uptime or speed to deployment rather than security.

Management

Often incentivized to not hear from security at all.



Five 9s Of Failure

A Lot Of This Is Beyond Our Ability To Change

But applying some empathy to understand motivations can go a long way.

Applying Empathy To Motivations

If someone’s actions or reactions are counter to security, applying empathy to understanding what motivates it can help.

When seeking the assistance of others, considering their motivations can help you frame your request in ways that makes the benefit clear to them.

Many Adventures Start In The Tavern

Share lunch with different teams in small groups to strengthen personal and professional relationships with them.

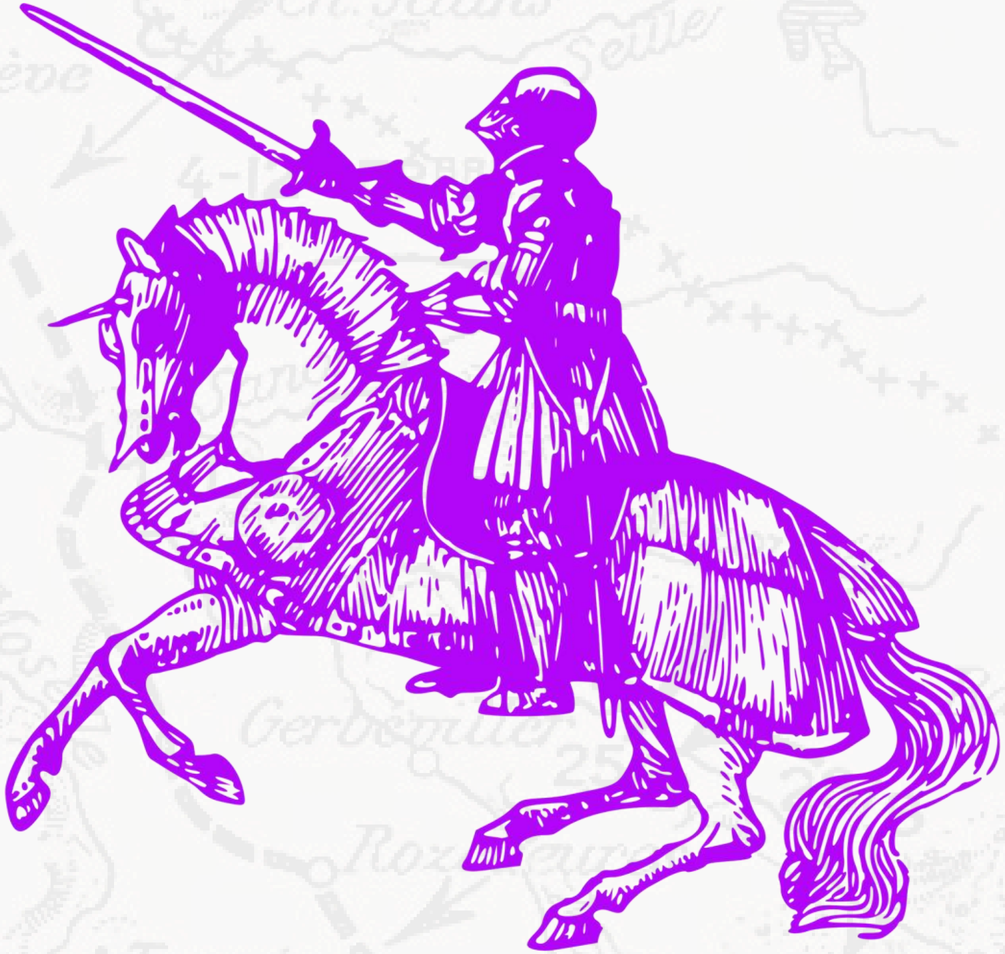
Saqueadores do Destino (Raiders of Fate) by LPVendetta
https://creativecommons.org/licenses/by-nc-nd/3.0/
https://www.deviantart.com/lpvendetta/art/Saqueadores-do-Destino-Raiders-of-Fate-7055 44478

Recruiting New Party Members

Creating good working relationships through the enterprise means more eyes and people with domain knowledge looking for risks.

Multiclass

Recruiting Security Champions boosts security throughout the enterprise.



Bringing The Party Together

Purple Team - Realignment

There is no separate Purple Team – it’s about having the Blue and Red Teams work together.

Both sides work to maximize the effectiveness of the other and work in a feedback loop.

The focus is increasing the security of the organization.

Isn’t This Obvious?

Focus On Time To Detection – **1/10/60**

A framework created by CrowdStrike

-1 minute to detect an intrusion
-10 minutes to investigate
-60 minutes to respond

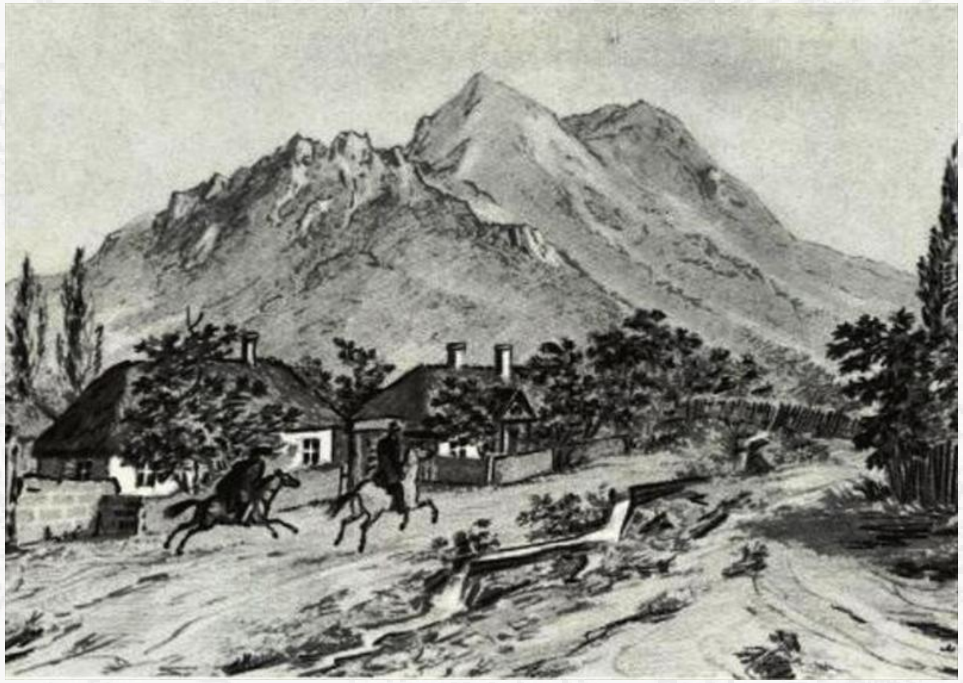
Breakout Times

https://www.crowdstrike.com/resources/reports/2019-crowdstrike-global-threat-report/

19 minutes	Russia
140 minutes	North Korea
240 minutes	China
309 minutes	Iranian
582 minutes	Criminals

Reducing Scope

One problem with large Purple Team exercises is they can show so many gaps that fixing them seems daunting.



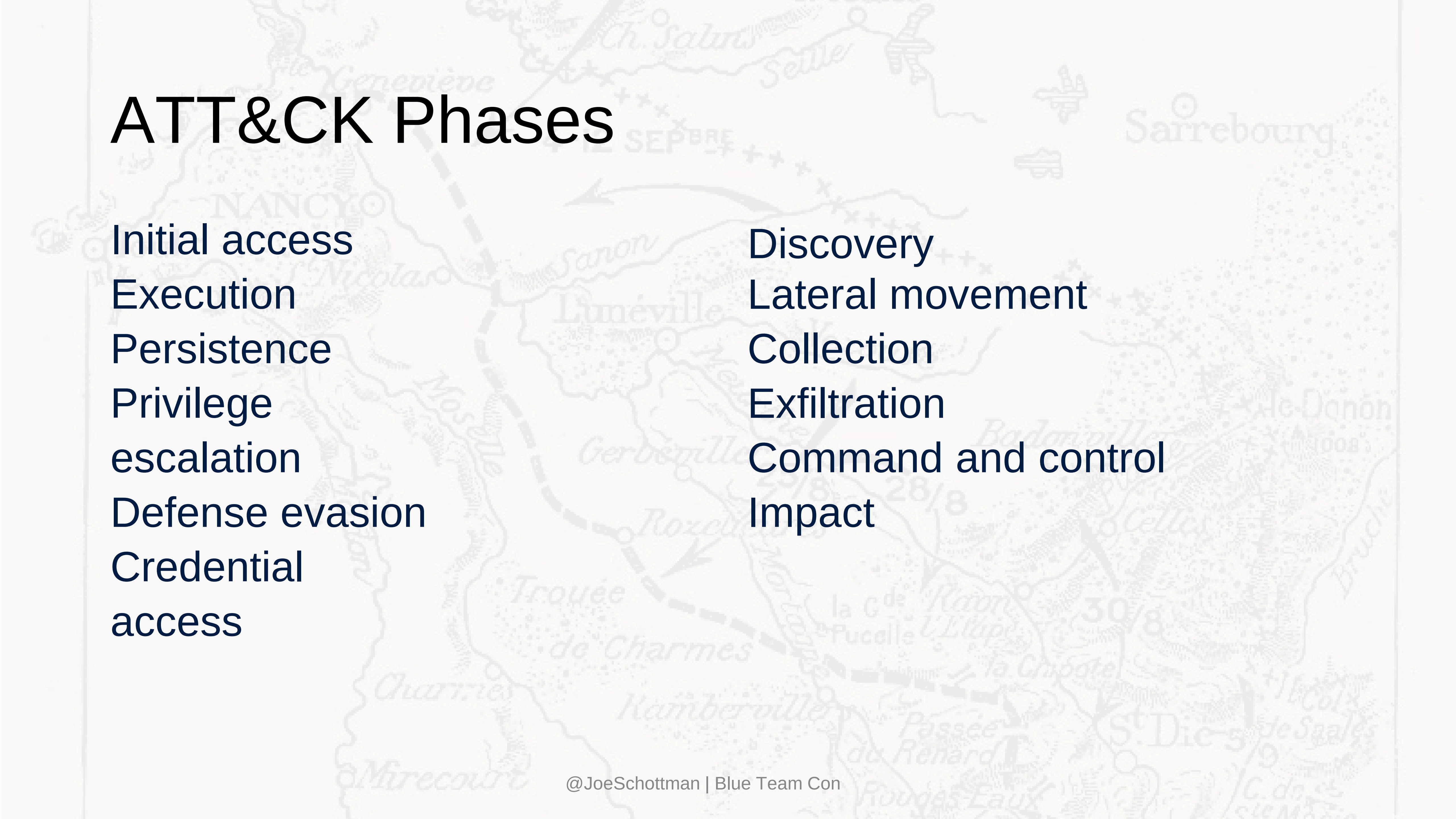
ATT&CK Matrix

Created by MITRE.

https://attack.mitre.org/matrices/enterprise/

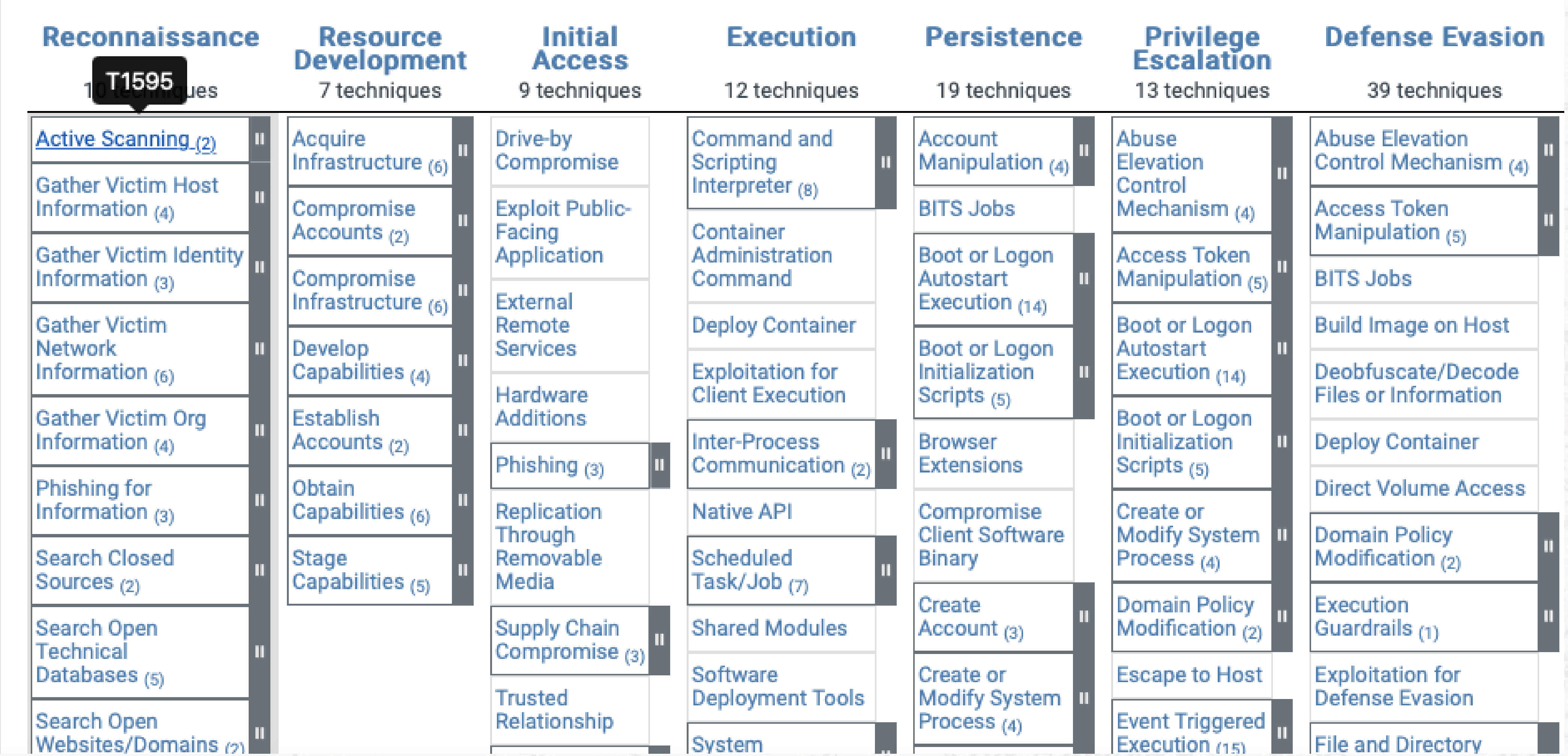
Breaks attacks into segments and then granularizes each segment with specific techniques.

ATT&CK Phases



- Initial access
- Execution
- Persistence
- Privilege escalation
- Defense evasion
- Credential access
- Discovery
- Lateral movement
- Collection
- Exfiltration
- Command and control
- Impact

The Matrix Has You



Reconnaissance

T1595

10 techniques

- Active Scanning (2)
- Gather Victim Host Information (4)
- Gather Victim Identity Information (3)
- Gather Victim Network Information (6)
- Gather Victim Org Information (4)
- Phishing for Information (3)
- Search Closed Sources (2)
- Search Open Technical Databases (5)
- Search Open Websites/Domains (2)

Resource Development

7 techniques

- Acquire Infrastructure (6)
- Compromise Accounts (2)
- Compromise Infrastructure (6)
- Develop Capabilities (4)
- Establish Accounts (2)
- Obtain Capabilities (6)
- Stage Capabilities (5)

Initial Access

9 techniques

- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing (3)
- Replication Through Removable Media
- Supply Chain Compromise (3)
- Trusted Relationship

Execution

12 techniques

- Command and Scripting Interpreter (8)
- Container Administration Command
- Deploy Container
- Exploitation for Client Execution
- Inter-Process Communication (2)
- Native API
- Scheduled Task/Job (7)
- Shared Modules
- Software Deployment Tools
- System

Persistence

19 techniques

- Account Manipulation (4)
- BITS Jobs
- Boot or Logon Autostart Execution (14)
- Boot or Logon Initialization Scripts (5)
- Browser Extensions
- Compromise Client Software Binary
- Create Account (3)
- Create or Modify System Process (4)

Privilege Escalation

13 techniques

- Abuse Elevation Control Mechanism (4)
- Access Token Manipulation (5)
- Boot or Logon Autostart Execution (14)
- Boot or Logon Initialization Scripts (5)
- Create or Modify System Process (4)
- Domain Policy Modification (2)
- Escape to Host
- Event Triggered Execution (15)

Defense Evasion

39 techniques

- Abuse Elevation Control Mechanism (4)
- Access Token Manipulation (5)
- BITS Jobs
- Build Image on Host
- Deobfuscate/Decode Files or Information
- Deploy Container
- Direct Volume Access
- Domain Policy Modification (2)
- Execution Guardrails (1)
- Exploitation for Defense Evasion
- File and Directory

Incentivize Control Validation

Networks and security controls and increasingly complicated.

If we’re lucky, we have a lot of capabilities to detect, contain, and mitigate, but how do we prove they work?

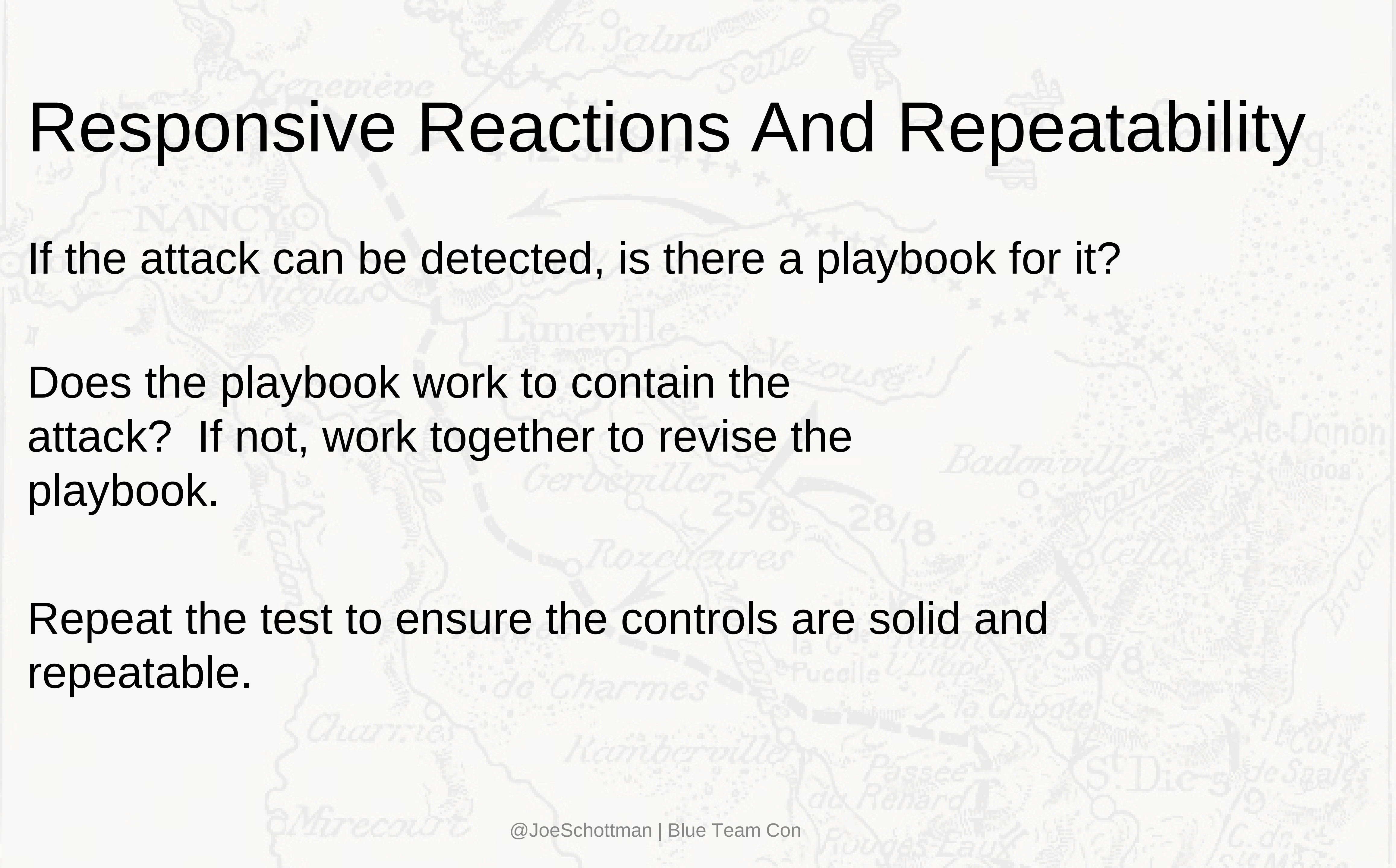
Control Validation can help and is something the red and blye teams can work together on.

Granular Tests

Red and Blue Teams work together to select specific attacks to test based on domain knowledge.

Test for detection and mitigation for that attack on all major network segments.

If the current infrastructure cannot detect an attack, work together to create signatures that can.



Responsive Reactions And Repeatability

If the attack can be detected, is there a playbook for it?

Does the playbook work to contain the attack? If not, work together to revise the playbook.

Repeat the test to ensure the controls are solid and repeatable.

Information Sharing

Both teams have knowledge that can help the other.

Breaking down silos enables more accurate testing and better controls.

The bad guys have time on their side; your organization has cooperation on its side.

Set Up A Cyber Range

Allow the Blue Team to step outside of “good” for a while.

Executing attacks can help understand them. Training provides an internal career path.

Pair Up For Exercises

Doing ride-alongs helps each team understand the challenges and experiences of the other.

Working side-by-side during exercises shortens the feedback loop.

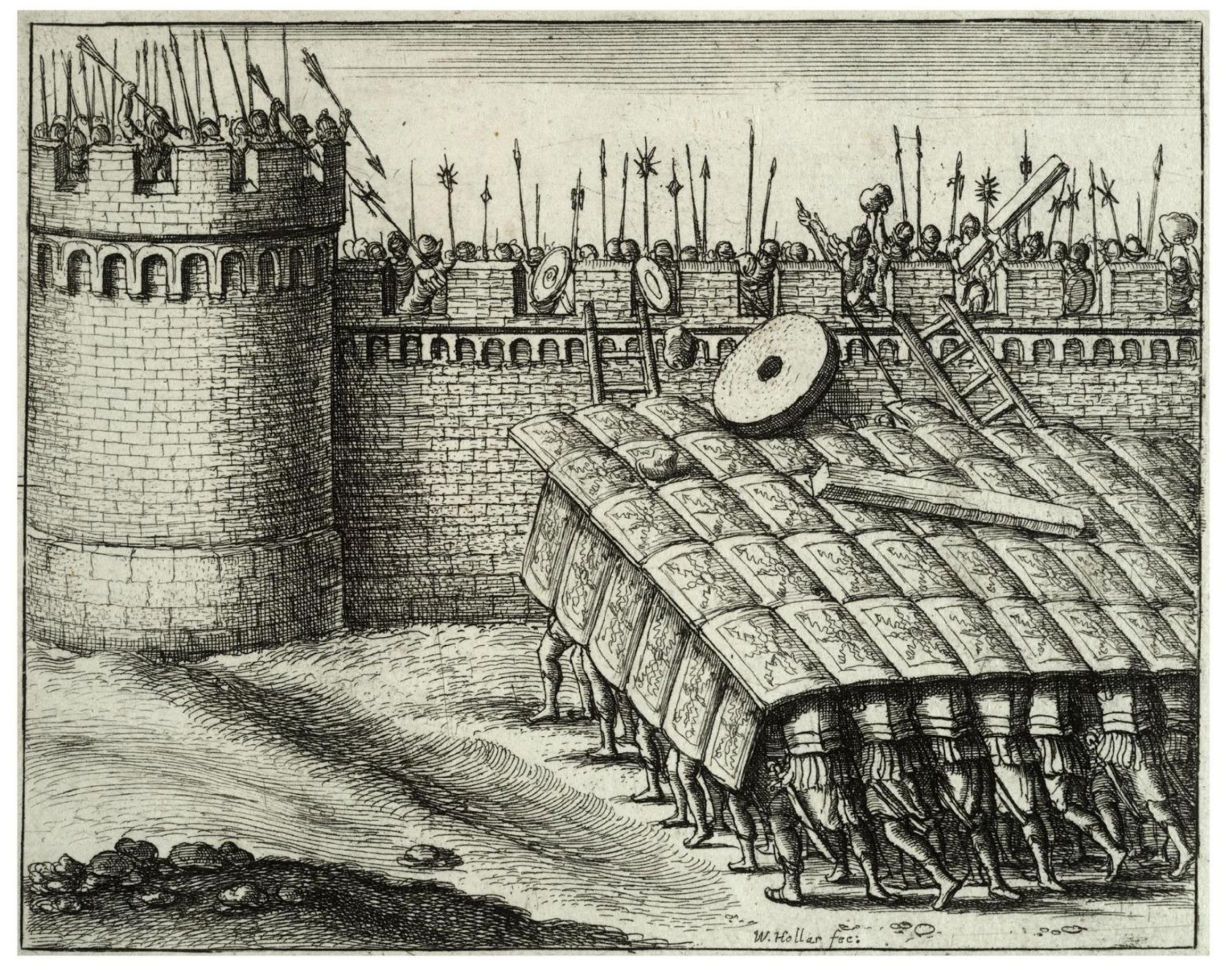
The Red Team learns the playbooks and can think of how to work around them. The Blue Team learns the Tactics, Techniques, and Procedures (TTPs) and how to detect them.

Strive For Synergies With IT

Development and Operations

- Include vulnerability remediation as a performance metric
- Push application testing left
- Provide feedback on logging during development
- Only require remediation of serious issues
- Deliver actionable reports, preferably directly to the tracking software

A Moment For The Humble Tank



What Is A Tank?

Massive Multiplayer Online Role Playing Game (MMORPG) characters that exist to take a lot of damage so the elite players can do the fun stuff.

SOC staff, especially junior analysts, often exist to do a lot of the grunt work that actually keeps enterprises secure so the elite staff can do the fun stuff.

Make Your Tanks Feel Appreciated

- Mentor them
- Explain rather than tell
- Push for training and advancement opportunities
- Say thanks

Ch. Salins
Seille
Geneviève
4-12 SEPBRE
Sarrebourg
NANCY
Toul
St Nicolas
Sanon
Lunéville
Vezouse
Meurthe
Moselle
Gerbéviller
25/8
28/8
Badonviller
le Donon
1008
Plaine
Celles
Rozelieures
Mortagne
la Gde Pucelle
Raon l'Étape
30/8
Trouée de Charmes
la Chipote
Charmes
Rambervillers
Passée du Renard
St Dié 5/9
Col de Saales
Bruche
Mirecourt
Rouges Eaux

Wrapping Up

Takeaways

- Explore what behaviors your company incentivizes, both for your team and others.
- Use empathy to understand what motives people.
- Realign bad incentives if you can.
- Ask “Does this security practice result in better security?”
- Break down silos so you can stay one step ahead of the bad guys.
- Take care of the people on the front line.

Questions? @JoeSchottman

Thanks to the board, the staff, and Volunteers!

Image Sources:

https://commons.wikimedia.org/wiki/File:Orc_mask_by_GrimZombie.jpg

https://en.m.wikipedia.org/wiki/Sta%C5%84czyk#/media/File%3AJan_Matejko%2C_Sta%C5%84czyk.jpg https://pixabay.com/vectors/bard-instrument-music-musician-1297201/

https://pixabay.com/illustrations/magic-magical-wizard-warlock-3216677/

https://pixabay.com/photos/fantasy-spirit-nightmare-dream-2847724/

https://commons.wikimedia.org/wiki/File:DnD_Dwarf.png

https://commons.wikimedia.org/wiki/User:LadyofHats#/media/File:DnD_Efreeti.png

https://commons.wikimedia.org/wiki/User:LadyofHats#/media/File:DnD_Ogre.png

https://commons.wikimedia.org/wiki/User:LadyofHats#/media/File:DnD_Basilisk.png

https://en.wikipedia.org/wiki/List_of_Dungeons_%26_Dragons_monsters_(1974%E2%80%9376)#/media/File:DnD_Griffon.png

https://en.wikipedia.org/wiki/List_of_Dungeons_%26_Dragons_monsters_(1974%E2%80%9376)#/media/File:DnD_Invisible_stalker.png https://en.wikipedia.org/wiki/File:DnD_Gnoll.png

https://en.wikipedia.org/wiki/List_of_Dungeons_%26_Dragons_monsters_(1974%E2%80%9376)#/media/File:DnD_gnome.png https://commons.wikimedia.org/wiki/File:Arthur-Pyle_The_White_Champion_meets_Two_Knights_at_the_Mill.JPG

https://commons.wikimedia.org/wiki/File:Carte_la_chipotte_001.jpg

https://commons.wikimedia.org/w/index.php?search=mountains+drawing&title=Special%3ASearch&go=Go&ns0=1&ns6=1&ns12=1&ns14=1&ns100=1&ns106=1#/media/File:Beshtau_Mountain_drawing_by_Mikhail_Lermontov_1837.jpg https://commons.wikimedia.org/wiki/File:DnD_Nixie.png

https://pixabay.com/photos/pillory-device-punishment-prisoner-51540/ https://cliparts.zone/clipart/1091064

https://en.wikipedia.org/wiki/File:Wenceslas_Hollar_-_A_testudo.jpg

https://en.wikipedia.org/wiki/Gargoyle_(Dungeons_%26_Dragons)#/media/File:DnD_Gargoyle.png https://upload.wikimedia.org/wikipedia/commons/d/d0/DnD_Orc.png