Realigning From Chaotic Evil

Joe Schottman
SANS Enterprise Summit
June 3, 2019
About Me

Senior Security Analyst for BB&T, Geek


GCIH, GCFA, GPEN, GWAPT

http://www.joeschottman.com/

@JoeSchottman on Twitter or add me on LinkedIn
Obligatory Disclaimer

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

All images are believed to be public domain, Creative Commons, or created for the presentation (including fair use by parody).
Additional Disclaimer

I’m not just talking about my employers.
And Yet Another Disclaimer

I’m not actually a D&D guru.
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 2019

<table>
<thead>
<tr>
<th>Challengers</th>
<th>Leaders</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced Persistent Dragons</td>
<td>Orcs</td>
</tr>
<tr>
<td>Win XP</td>
<td>Bag of Containers</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Lich Players</th>
<th>Visionaries</th>
</tr>
</thead>
<tbody>
<tr>
<td>COBOL</td>
<td>Gelatinous Kube</td>
</tr>
</tbody>
</table>

Bigness of teeth

Number of sharp, pointy things

©Gandalf
Gandalf Magic Quadrant

Cyber Threats 2019

Leaders
- Advanced Persistent Dragons

Challengers
- Orcs
- Bag of Containers

Lich Players
- Win XP
- COBOL

Visionaries
- Gelatinous Kube

Number of sharp, pointy things

Bigness of teeth

© Gandalf
No, Seriously, Why Am I Giving This Talk?
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.
Skoudo Baggins
Corrupted by the One Ring ($\Theta$)
Becomes the King In Yellow
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@N02/11622384283/in/photostream/
With These
Or You Get This

Marco Hazard
Lego Fantasy Scenery - They Can't Co-exist
https://creativecommons.org/licenses/by-sa/2.0/
https://www.flickr.com/photos/42405591@N02/11622515344/
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
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
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
• Not appearing in newspapers as having been owned
Developers

Often incentivized by new features rather than stability or security.
Operations

Often incentivized by uptime or speed to deployment rather than security.
Five 9s Of Failure
A Lot Of This Is Beyond Our Ability To Change
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-705544478
Recruiting New Party Members

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


19 minutes for Russian APTs
140 minutes for North Korean APTs
240 minutes for Chinese APTs
309 minutes for Iranian APTs
582 minutes for 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
| Initial Access                  | Execution                  | Persistence                  | Privilege Escalation     | Defense Evasion | Credential Access | Discovery                  | Lateral Movement | Collection | Command and Control | Exfiltration | Impact                  |
|--------------------------------|-----------------------------|------------------------------|--------------------------|-------------------|-------------------|-------------------|--------------------------|--------------|------------|---------------------|-------------|------------------------|
| Drive-by Compromise            | AppleScript                 | .bash_profile and .bashrc   | Access Token Manipulation| Access Token Manipulation| Account Manipulation| Account Discovery | Audio Capture            | Commonly Used Port | Automated Exfiltration | Data Destruction |
| Exploit Public-Facing Application | CMSTP                      | Accessibility Features      | Accessibility Features   | BITS Jobs          | Bash History       | Application Window Discovery | Application Deploymen tSoftware | Automated Collection | Communication Through Removable Media | Data CompressedD |
| External Remote Services       | Command-Line Interface      | Account Manipulation        | AppCert DLLs             | Binary Padding     | Brute Force       | Browser Bookmark Discovery | Distributed Component Object Model | Clipboard Data | Connection Proxy | Data Encrypted             | Data Encryption for Impact |
| Hardware Additions             | Compiled HTML File          | AppCert DLLs                | AppInit DLLs             | Bypass User Account Control | Credential Dumping | Domain Trust Discovery | Exploitation of Remote Services | Data Staged | Custom Command and Control Protocol | Data Transfer Size Limits |

Joe Schottman | SANS Enterprise Summit | June 3, 2019
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.
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 Similar Synergies

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
Wrapping Up
Takeaways

Explore what behaviors your company incentivizes, both for your team and others.

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