Red (Purple) Blue ->
Collaboration for optimum results

SANS Purple Team Summit 2019
Prithvi Bhat
Prithvi Bhat

Blue teamer – focus on building SOC, purple teaming, MSS delivery and incident response.

Travel enthusiast – Lived in 4 countries and travelled to more than dozen countries.

Ardent philosopher – Reading and having conversation with people of varied interests and background.
Pillars of cybersecurity

- Threat Intelligence
- Red team (offensive security)
- Blue team (defensive security)
- Incident response
Battling in silos
We all are a family with a helpful neighbor

Red team
Threat Intel
Blue team

MITRE ATT&CK
Combining strengths for better security

**RED TEAM**
Realistic, simulated attack, following the profile of an actual threat actor to the organization. The red team will try and achieve a number of agreed objectives without raising any detection or response.

**BLUE TEAM**
Continuous monitoring of and response to indicators of attacks and compromises. To this end, the blue team establishes and improves on detection measures in the IT infrastructure and defines and implements specific “use cases” to monitor for.

**PURPLE TEAM**
Combining the red and blue team efforts in an interactive setting: by performing an attack while the blue team is actively watching which elements are and are not detected. Afterwards, both blue and red team improve their approach and retry.
Make friends with the helpful neighbor

1. Threat Intelligence
2. Tailor the scenario
3. Execute the attack scenario
4. Monitor within the SIEM/SOAR/?

MITRE ATT&CK MATRIX
Gain threat intelligence on attacks to similar companies

Identify an attack scenario mapped to ATT&CK

Execute the attack scenario

Monitor within the SIEM/SOAR/

Evaluate attack and identify gaps in detection

Develop additional detection methods, request additional logging

Replay the attack scenario

Exercise complete

TIBER style purple teaming
Collaboration benefits

• Intel for the benefit of red and blue team.

• Red and blue team together for a solid purple team.

• Purple team for the benefit of incident response team.
Summary

• Its hard! Yet simple 😊
• More realistic detection
• Better understanding of threat actors’ TTPs
• Cross domain knowledge
• Building relations with other teams
• Improving capabilities throughout
Next steps

• Is your organization doing red team exercises?
  If red team = no
  - Push for red team and get involved
  Else
  - Get involved

• Does your red team and blue team leverage threat intel?
  - If not, start collaborating

• Evolve from red team to purple team

• It will show more value
  - Better incident response