Thinking Purple

Who am I

- Contributor to several security projects and initiatives:
  - Multiple Open Source Projects (PowerShell, Python, Ruby ..)
  - Metasploit Framework
  - PTES (Penetration Execution Standard
  - Obsidis Consortia/ Init 6 / BSides PR
- Microsoft MVP
- Work as a Director of Reverse Engineering for a security vendor
- Podcaster

Agenda

- What is Red
- What is Blue
- What is Purple
- Current Situation
- Engagements Type
- General Recommendations
- Metrics

What is Red?

A internal **independent** team that performs emulation of **adversarial tactics, techniques and procedures (TTPs)** to test plans and systems the way they may actually be defeated by aggressors; to **challenge** plans and **improve** decision making processes.

- Justin Warner (@sixdub)

What is Red?

- Research and information dissemination on attackers TTPs and threats
- Conduct
  - Cooperative Engagements
  - Threat Simulation
  - Adversary Emulation
  - Full Scope Attack Simulation
- Risk assessment of new technologies

What is a Blue?

The blue team is the team **responsible** for **monitoring** and **defending** an **organization's information assets** including **investigating and remediating security incidents.**

- Dave Hull (@davehull)

What is a Blue?

- Hunts in the network for IOCs (Indicators of Compromise) to detect attacks in all of their stages both internally and externally.
- Develop, update and validate incident response plans and procedures.
- Work with stakeholders and management on creation, updating and testing of breach recovery plans.
- Works with red team to validate new risks that come from new techniques and tools.

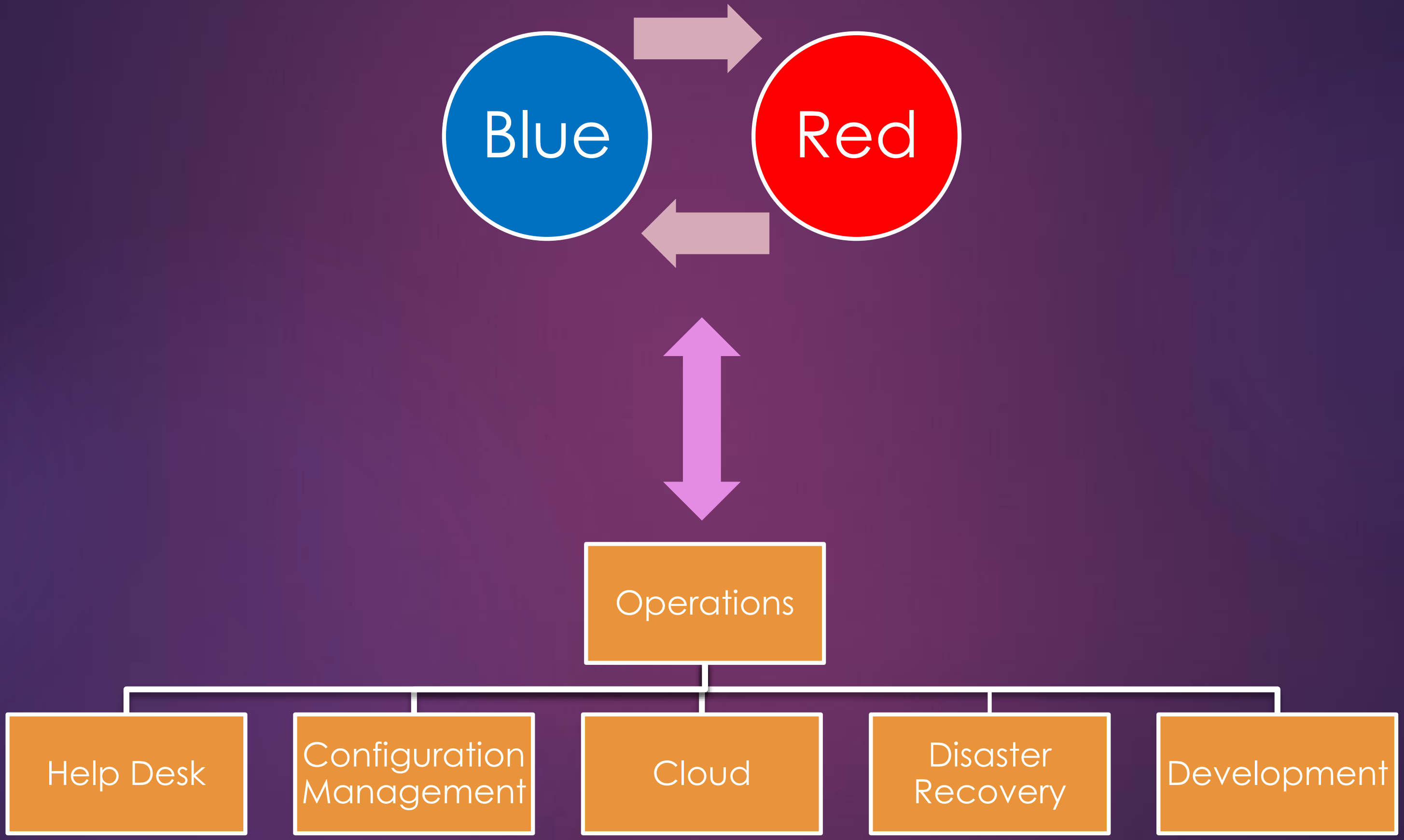
What is a Blue?

- Works with operations:
  - Developing, updating and validating breach recovery plans.
  - Developing, updating and implement secured and monitored configurations.

What is Purple?

- Purple is the symbiotic relation between Red and Blue team in a way that improves the security of the organization, constantly improving the skills and processes of both teams.
- Red Team operates in a open manner in terms of results and TTPs used so Blue can improve its techniques.
- Blue informs of what was detected and why, improving Red techniques and pushes for improved TTPs.
- Red provide blue with the evidence to back recommendations and changes to ops.

What is Purple?



Blue

Red

Operations

Help Desk

Configuration Management

Cloud

Disaster Recovery

Development

Current Situation

Current Situation

- Many Red and Blue teams lack the buy in from management.
- Lack of empathy or tact when delivering results, Red to Blue, Blue to Operations.
- Many Red Teams become or are forced to be institutionalized.
- We find Tribalism between security teams where there is a level of mistrust and lack of cooperation.
- Evaluation methods of each one of the security teams rewards one team beating the other.

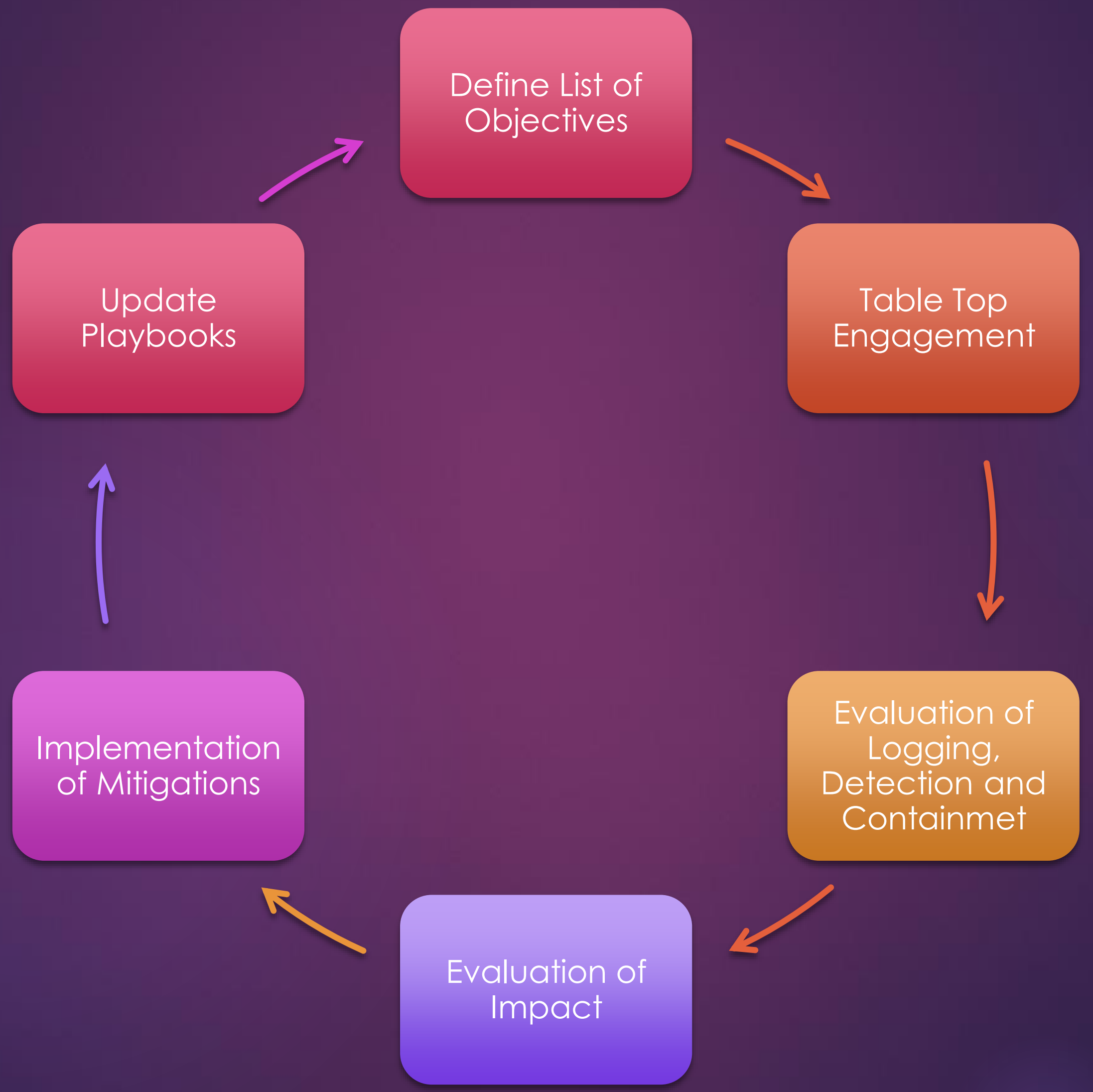
Current Situation

- Red Team both internal or contractor as seen as a check mark and not for the risk mitigation value they provide.
- Red Team has a limited bag of tricks becoming predictable. Many times lacks the skill to expand it.
- Blue Team is tool bound lacking the ability to adapt and modify tool set.

Engagement Types

THE RIGHT ONE FOR THE RIGHT OUTCOME

Cooperative Engagement



Define List of Objectives

Table Top Engagement

Evaluation of Logging, Detection and Containmet

Evaluation of Impact

Implementation of Mitigations

Update Playbooks

Cooperative Engagement Execution

- Engagement is performed with both Red and Blue team communicating action between each other.
- Red communicates each action taken so Blue can test detection and IOCs.
- Blue allows Red to continue and documents what IOCs were detected, which where not and possible containment/remediation steps.
- A debrief is done to validate all steps taken to determine attack graph, areas where detection should have happened and creation/validation of containment approach.

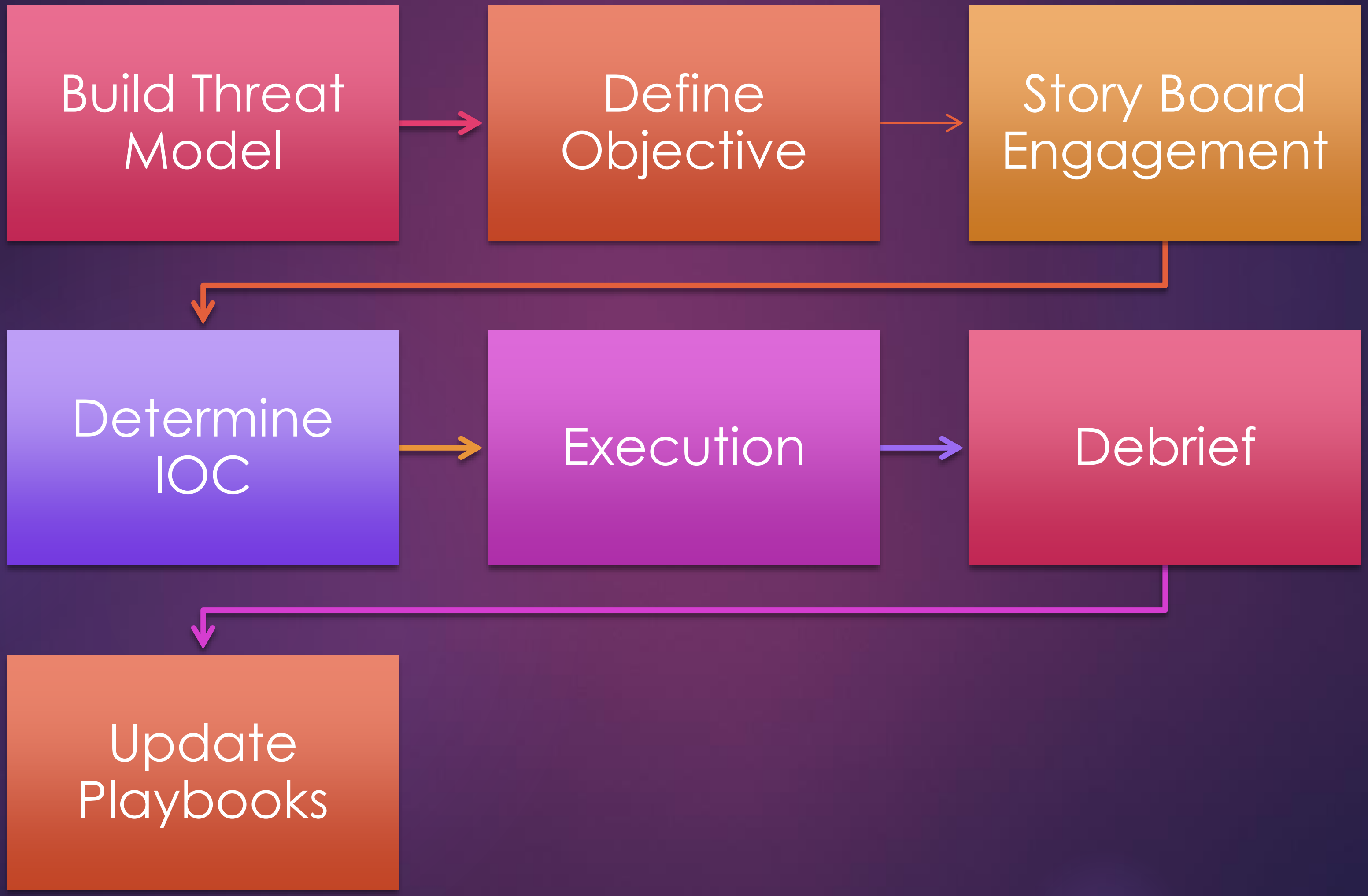
Cooperative Engagement Execution

- Impact of overall threat is evaluated and broken in to individual system or areas of impact so as to evaluate remediation and recovery plans for each area.
- Incident Response and Remediation Playbooks and knowledge base are updated. Red does the same.

Cooperative Engagement Main Considerations

- This type of engagement is preferred for:
  - Start of a program.
  - Analysis phase of a new technology.
  - Best value on effort for small entities.
  - Heavily constrained environments.
- Engagement is performed with both Red and Blue team communicating action between each other.
- The engagement starts with a clear set of goals as to what will be executed for validation of processes and techniques.
- Engagement can be as limited as detection of OSINT exposed or to an Insider Threat.

Threat Simulation



Threat Simulation Execution

- Build a threat model based on news and/or threat intelligence.
- Create a "storyboard" of actions based on the general TTPs of the known threat.
- Determine what would be the common IOCs that the specific threat would create on the traversed and affected systems.
- Execute actions storyboarded for the threat.
- Debrief to identify gaps, mitigations and analisys.
- Incident Response and Remediation Playbooks are updated. Red updates their attack knowledge base.

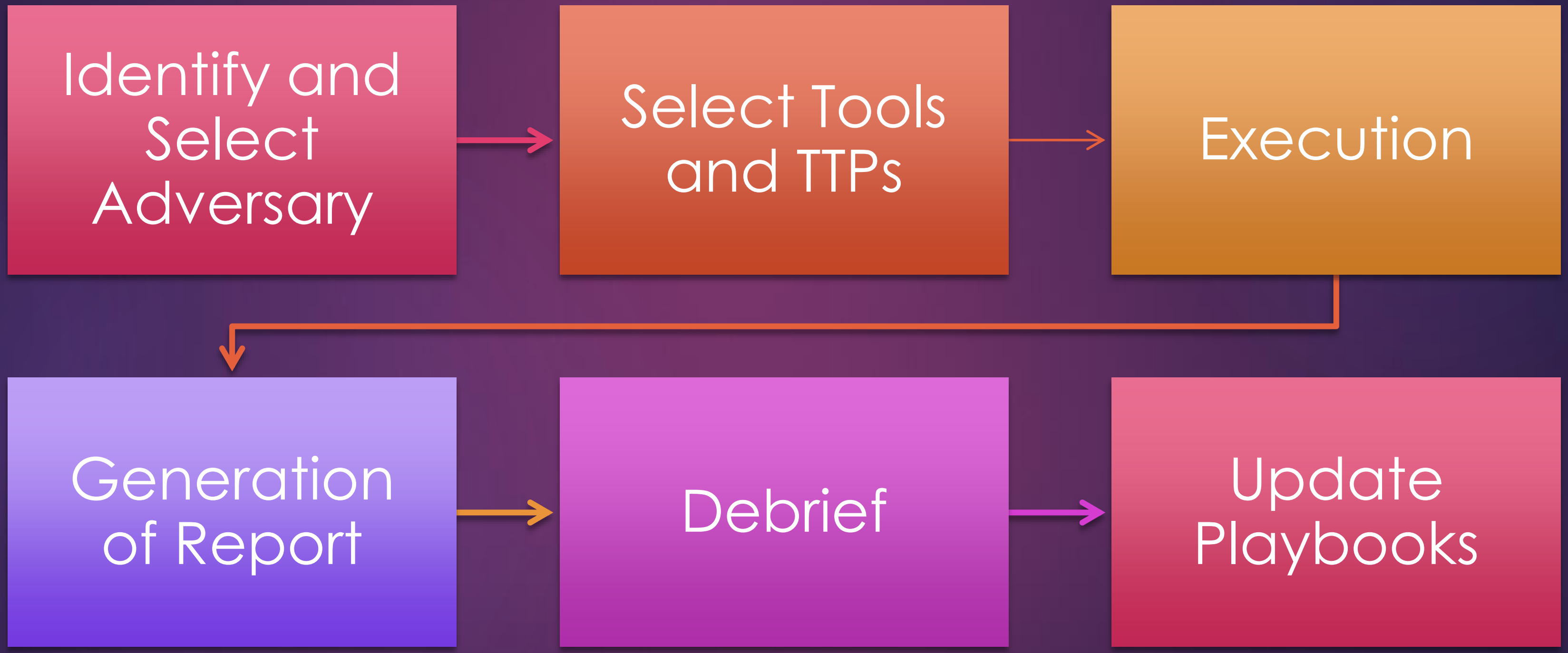
Threat Simulation Execution

- Execute actions storyboarded for the threat.
- Debrief to identify gaps, mitigations and analisys.
- Incident Response and Remediation Playbooks are updated.
- Red attack playbooks are updated.
- Report on recommendations to Operations and other parties.

Threat Simulation Main Considerations

- The threat model will determine what is the level sophistication for the TTPs that will be storyboarded.
- The threat model may include physical security, social engineering and/or technical operations that will be conducted.
- TTPs are selected by impact and likelihood since more often than not, all possible TTPs for a threat model can't be exercised due to:
  - Time Constraints
  - Resource Constraints
  - Operational Constraints
  - Political Constraints

Adversary Emulation



Identify and Select Adversary

Select Tools and TTPs

Execution

Generation of Report

Debrief

Update Playbooks

Adversary Emulation Execution

- Information on the adversary is already known (TTPs, Tools..etc)
- Tools are selected, modified and TTPs stablished that will mimic the IOCs generated by the adversary.
- Engagement is executed as a full assessment with no prior warning to test detection, mitigation and containment plans.
- At the end of the exercise a full report of actions and goals achieved is prepared and Blue is informed.

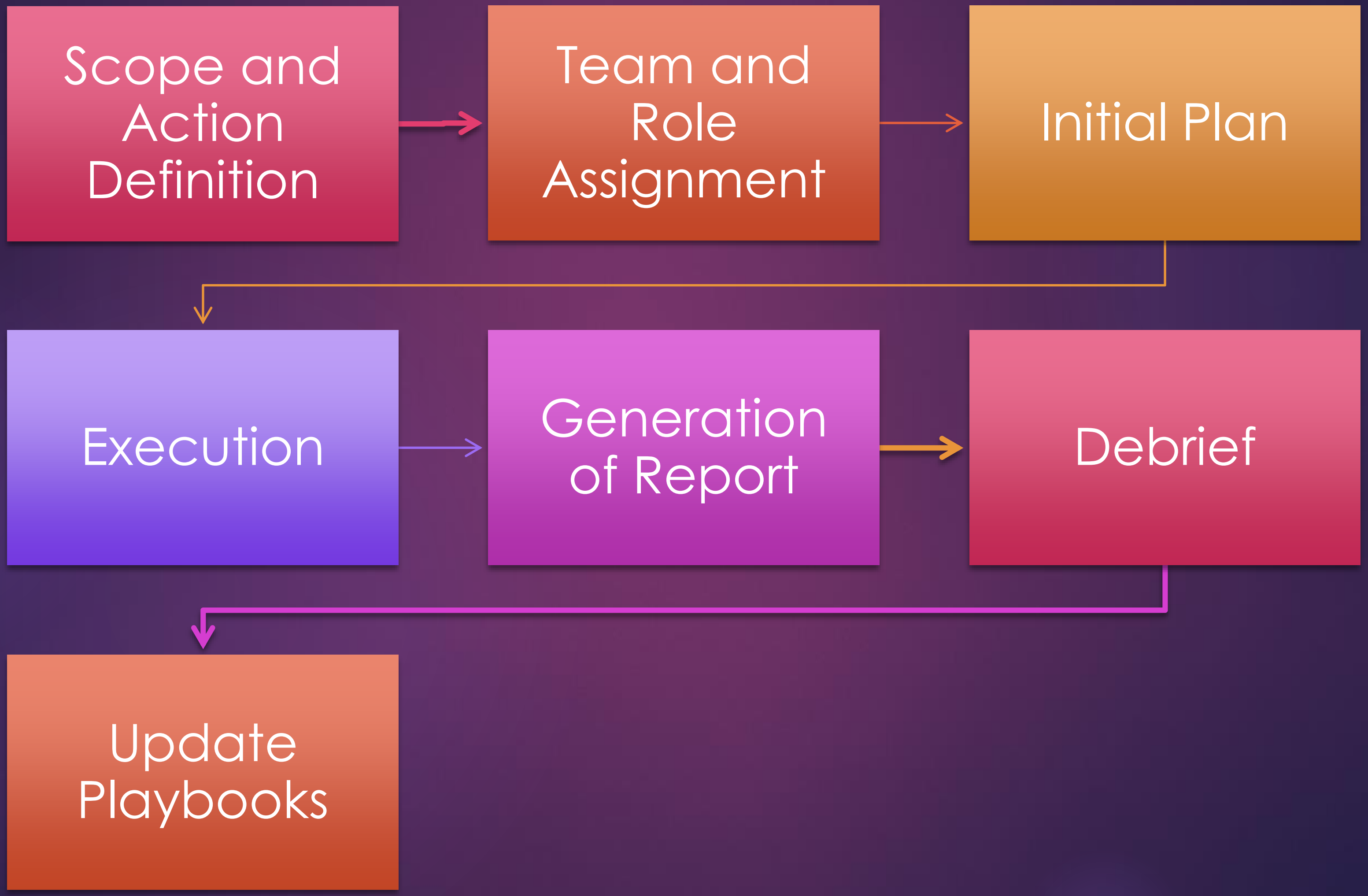
Adversary Emulation Execution

- Summary of the report is given to Blue before full debrief
  - Adversary that was emulated.
  - Source IPs for C&C and Pivot Actions.
  - Targeted Systems.
- Full Debrief is performed.
- Incident Response and Remediation Playbooks are updated. Red updates their attack playbooks.
- Report on recommendations to Operations and other parties.

Adversary Emulation Main Considerations

- Main goal is to test detection, containment and remediation of a known attacker.
- Since adversary should already be a known one no prior warning should be given to Blue.
- Ensure that tools generate the same IOCs on host and network as the ones known by the adversary emulated.
- A summary of the report is sent ahead of full debrief, purpose is so Blue can review and come with a list of what was found and missed.

Full Scope Attack Simulation



Scope and Action Definition

Team and Role Assignment

Initial Plan

Execution

Generation of Report

Debrief

Update Playbooks

Full Scope Attack Simulation Execution

- Scope and Define goals of simulation:
  - Physical Red Team
  - Social Engineering
  - Technical
- Assign roles and areas of focus to team members if size of team allows for specialized tasks.
- Create an initial attack plan for each goal and rules of engagement to follow.
- Execute initial plan of action.
- Validate results and re-orient as more information is available and actions taken.

Full Scope Attack Simulation Execution

- Internal Red Team debrief of actions taken, goals achieved and failed.
- Prepare and send summary to Blue team for final debrief.
- Debrief with Blue.
- Blue identifies areas of success and areas of technical improvement.
- Incident Response and Remediation Playbooks are updated.
- Red attack playbooks are updated.
- Report on recommendations to Operations and other parties.

Full Scope Attack Simulation Main Considerations

- Engagement is executed with no prior warning to the blue team.
- TTPs should be varied and should be in accordance to the level of simulation set in the initial scope and goals.
- Constant update to a project manager or team lead is critical to coordinate actions and prevent any accidental mishap.
- A list of emergency phones and channels of communications must be defined and kept in case of needed to stake holders.

Full Scope Attack Simulation

- As part of the action the identification of possible detection and actions to contain should be looked for and noted.
- Teams should be rotated so as to maintain proficiency on all areas of specialty across the team.
- Ensure that no standard TTPs and IOCs are developed and that constant sanitation evaluations are done of the toolset and TTPs as possible.
- Ensure that exfiltration of confidential and IP data is secured in transit and storage.
- Ensure to curtail destructive actions or risky action against business critical systems.

Recommendations

Recommendations

- Without buy in from the key people that can push for change it is a hard battle for both teams.
- Management and team members must be willing to hear bad news and have fines when delivering them.
- Don’t Red Team too death by performing to frequent full scale assessments.
- Don’t Blue Team operations to death asking for changes in a tempo that does not matches the changes of the environment.

Recommendations

- Red Team value is their ability to think outside the org mentality, avoid assimilation to the corp culture but still understand it.
- A constant training of both sides and cross training should be done.
- One has to break the tool centric mentality in both teams. They should be able to adapt existing and build their own.
- Control of egos on both sides both internal and across teams is critical. Good to have a Devil's Advocate but not a saboteur.

Metrics

YOU CANNOT MANAGE WHAT YOU CANNOT MEASURE

Recommendations Metrics Purple

- Metrics should not be ones where the success of one team is the failure of another.
- Measure the number of recommendations and actions on both teams that come from each engagement.
- Measure number of interactions between teams outside of the engagements.
- Measure the amount of simulations conducted between Red and Blue.
- Measure their interactions as a security org with Operations and other teams.

Recommendations Metrics Red

- Number of engagements and type performed.
- Tools written and updated to existing tools.
- Number of gaps identified.
- Number of updates to playbooks and shared knowledge base and quality of contribution.

Recommendations Metrics Blue

- Keep of metric on discoveries when they are informed to ops, how long before they are addressed and how long before it is seen in attacks.
- Numbers of incidents handled.
- Number of malware sample analyzed.
- Number of updates to playbooks and shared knowledge base.
- Time to Detect
- Time to Remediation

KEEP
CALM
BECAUSE
WE ARE THE
PURPLE TEAM

Big Thanks!

- Dave Hull (@davehull) Tanium
- Justin Warner (@sixdub) Veriss Group
- Jessica Payne (@jepayne) Microsoft
- Sean Metcalf (@Pyrotek3) Trimarc

Thank You!

@carlos_perez

http://www.darkoperator.com

References

- http://redteamjournal.com/about/red-teaming-and-alternative-analysis/
- https://digital-forensics.sans.org/summit-archives/Prague_Summit/Blue_Team_Perspectives_David_Kovar.pdf
- http://redteamjournal.com/2016/02/red-teaming-and-the-library-of-babel/
- http://redteams.net/blog/
- https://medium.com/starting-up-security/red-teams-6faa8d95f602#.8w3iycxt2
- https://community.rapid7.com/community/infosec/blog/2016/06/23/penetration-testing-vs-red-teaming-the-age-old-debate-of-pirates-vs-ninja-continues

References

- https://www.sixdub.net/?p=705
- http://www.darkoperator.com/blog/2015/11/2/are-we-measuring-blue-and-red-right
- http://redteamjournal.com/2016/07/the-dangerous-illusion-of-certainty/
- http://www.dtic.mil/doctrine/notes/jdn1_16.pdf
- http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
- https://www.mitre.org/sites/default/files/publications/pr_14-3929-cyber-exercise-playbook.pdf