ATOMIC PURPLE TEAM

IDEN0011.1

Atomic Purple Team Lifecycle

- Ingest
- Plan
- Attack
- Hunt
- Defend
- Report

APPLIED
PURPLE
TEAMING

Infrastructure
Threat Optics
Continuous Improvement

ISACA®
Trust in, and value from, information systems
Denver Chapter

DEFENSIVE
ORIGINS

BLACK HILLS
Information Security
• 2008 •

Ok, NIST? Blue Team.

- Responsible for **defending** an enterprise’s use of information systems by maintaining its security posture…
- **Identifies** security threats and risks in the operating environment, **analyzes** the network environment and its current state of security readiness.
- **Provides recommendations** … to increase the customer's cyber security readiness posture.

https://csrc.nist.gov/Glossary/Term/Red-Team-Blue-Team-Approach

Ok, NIST? Red Team.

- **Emulate** a potential adversary’s **attack** or **exploitation**
  - Systems / Services
  - Personnel
  - Facilities / Vehicles
- Improve enterprise Information Assurance by **demonstrating the impacts** of successful attacks
- **Demonstrating** what works for the defenders

https://csrc.nist.gov/Glossary/Term/Red-Team-Blue-Team-Approach

Red Team, Blue Team, Purple Team

Red Team: Offense. Attack. Pillage.

Blue Team: Defense. Block. Build.

Purple Team: Collaboration of Red and Blue Teams.

- Attack, Defend, Pillage, Build.
- Use both Blue Team and Red Team tactics to increase efficiency of Security Posture improvement programs.

https://csrc.nist.gov/Glossary/Term/Red-Team-Blue-Team-Approach

Who/What is APT? Where does it fit?

- Some organizations have Blue and Red Teams.
- Some organizations have just Blue, or Red teams.
- Some organizations have neither Blue or Red teams…
- Consider Network Analysts and a Help Desk.
- MSP’s, MSSP’s

The **Purple Team** can be an independent team, multiple teams, a few employees, or single employee; It works best as a team of **collaborative effort** from **Information Security** related departments and roles.

It can fall under Information Security, Information Technology, or cross organizational unit to leverage collaborative effort..

Atomic Purple Teaming

What does an APT accomplish?

- Build a more secure business infrastructure
- Align Information Technology infrastructure to best practices
- Keep businesses protected by monitoring current threats
- Assess risk and threats of vulnerabilities
- Build and implement effective defenses and alerting methods

Atomic Purple Team & Production - Lifecycle

The APT does not operate in production environments.

- Lab Environment used to test attacks, test defenses, test changes.

The goal of APT is to:

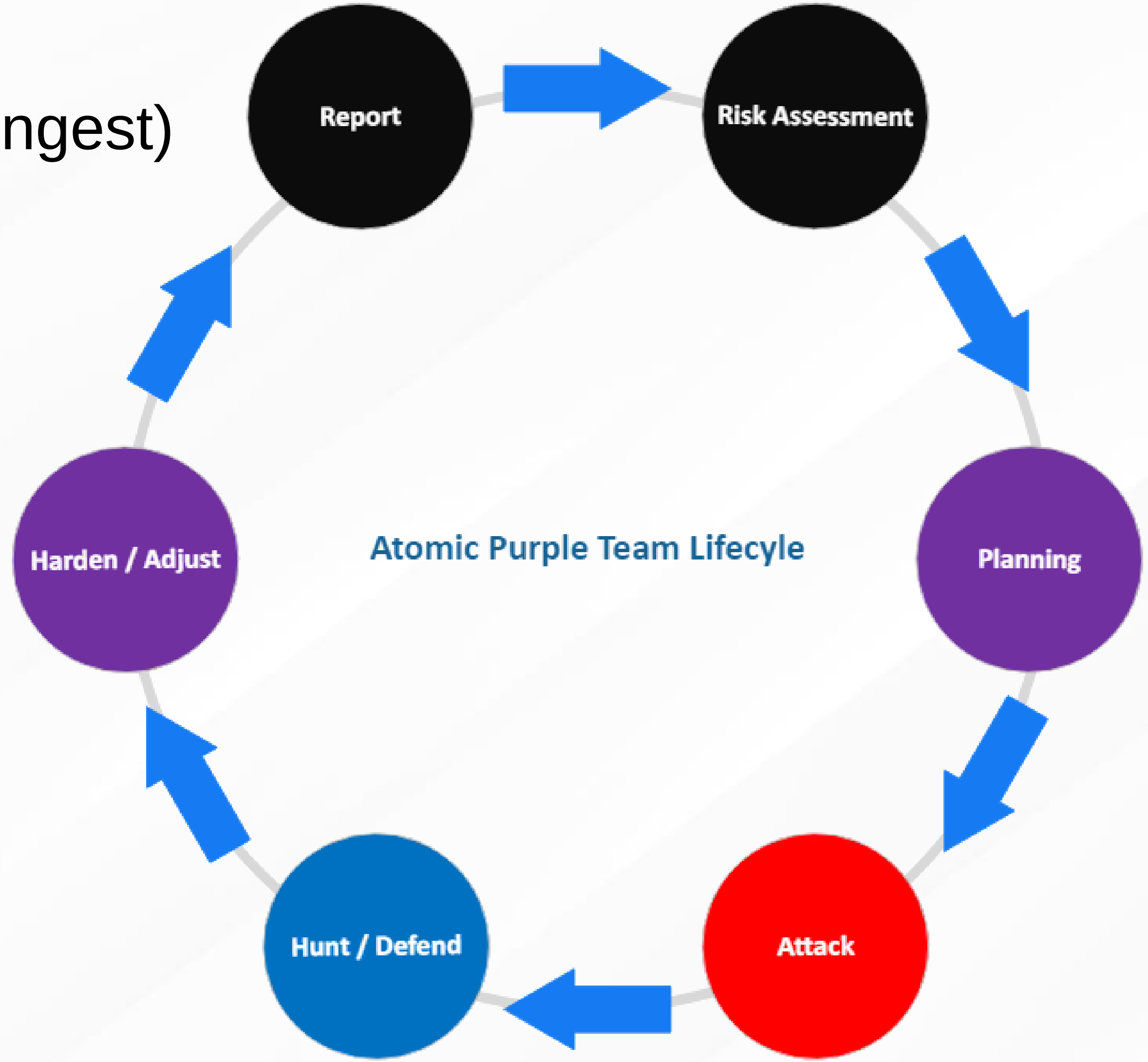
- Produce proven methods to defeat attacks
- Identify/alert threats
- Continually improve the security posture of the organization

DO NOT TEST IN PRODUCTION.

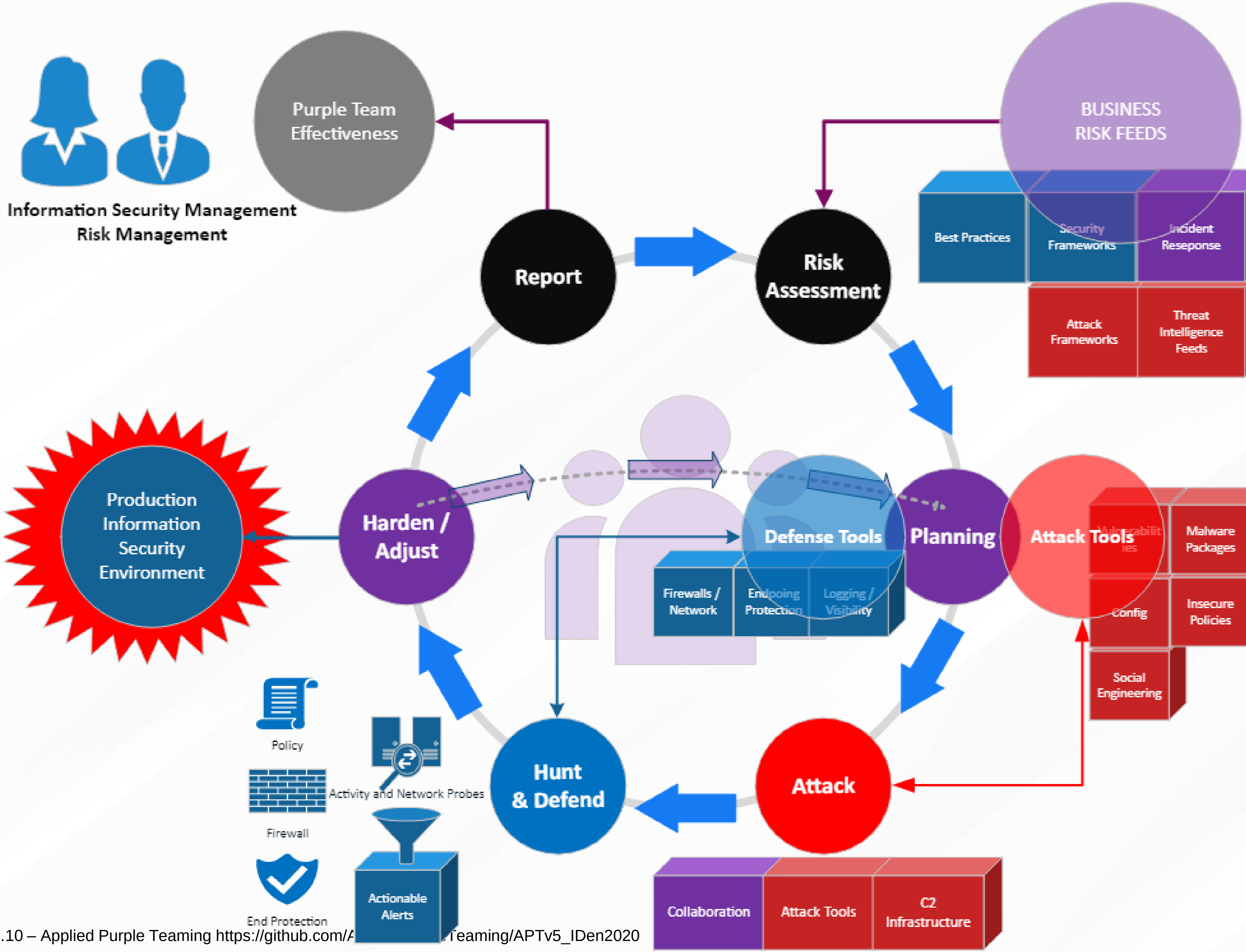
APT produces proven methodologies with empirical evidence for production Change Management by testing in a lab/simulated environment!

Applied Purple Team Lifecycle

1. Risk and Threat Assessment (Attack Ingest)
2. Planning
3. Attack Execution / Simulation
4. Detection / Build Defenses
5. Optimize / Harden / Adjust
6. Report



APTLC
Big (Macro) Picture



ATOMIC PURPLE TEAM

defensiveorigins.com

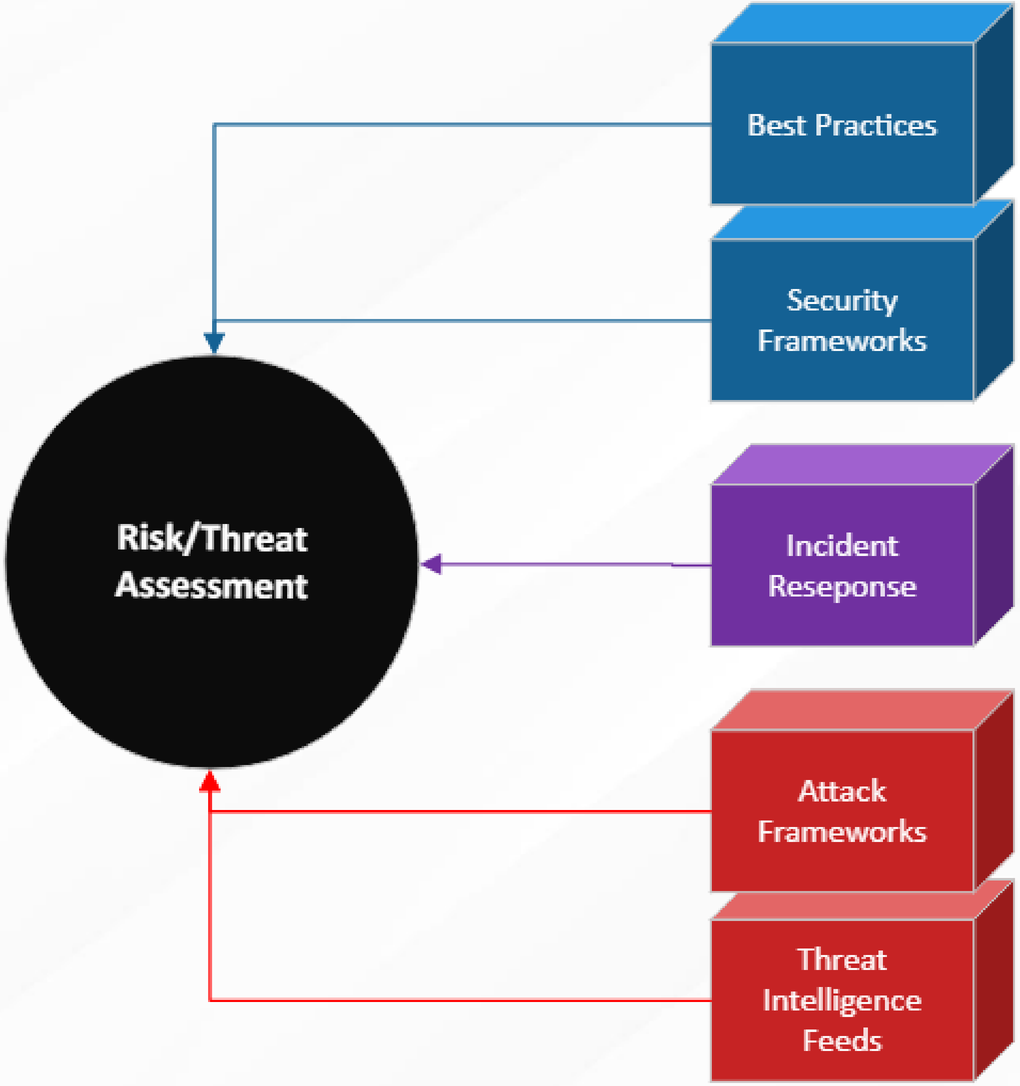
1. Risk and Threat Assessment / Attack Ingest

Goal: Find an attack.

Goal: Determine if defending and/or hunting

How: Use an ingest:

- Best Practices (audit)
- Security Framework
- Current Events
- CLR / DLR / Boo / .NET
- Incident Response
- Threat Intelligence



defensiveorigins.com

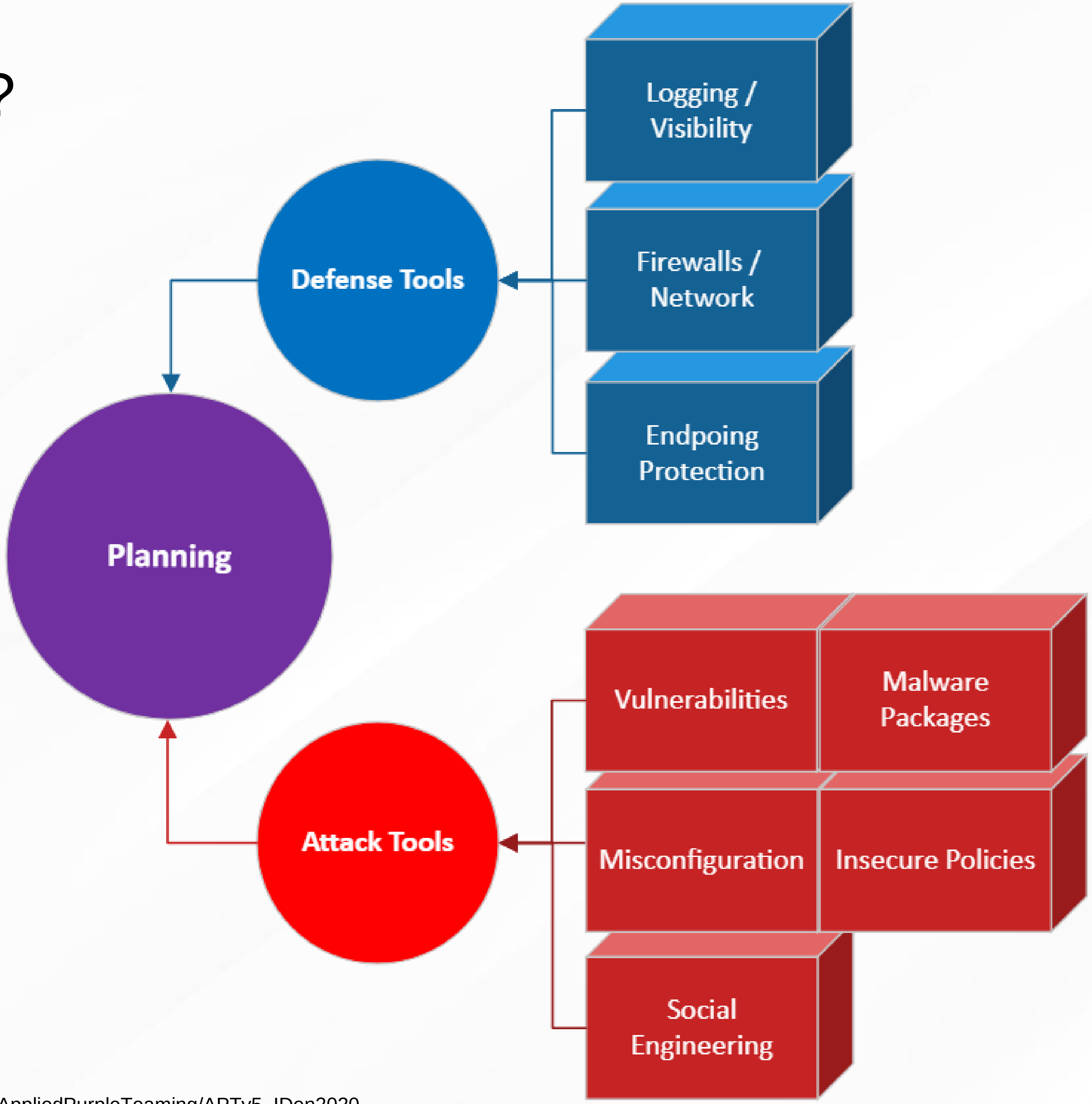
2. Planning – What are the Tools?

Goal: Identify the Attack Tools

Goal: Identify the Defense Tools

How:

- Provided by Threat Assessment
- Research
- New tools?? Great!!



ATOMIC PURPLE TEAM

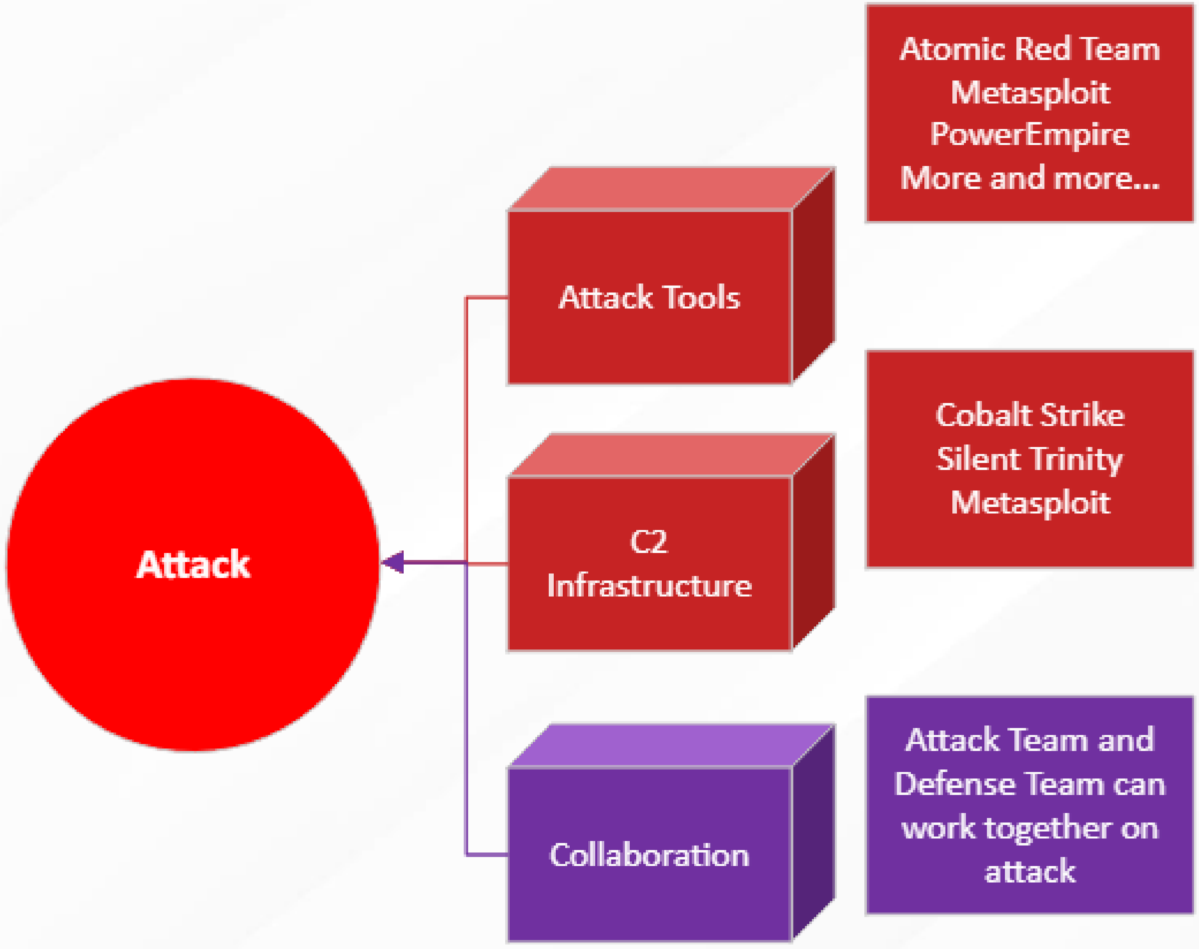
defensiveorigins.com

3. Attack / Execute / Engage

Goal: Execute the attack.

What attacks were successful?
What data could be found?
Was a pivot possible?
Could a C2 be achieved?

Did the attack achieve its goal?
Why? Why not?



4: Hunt and Defend

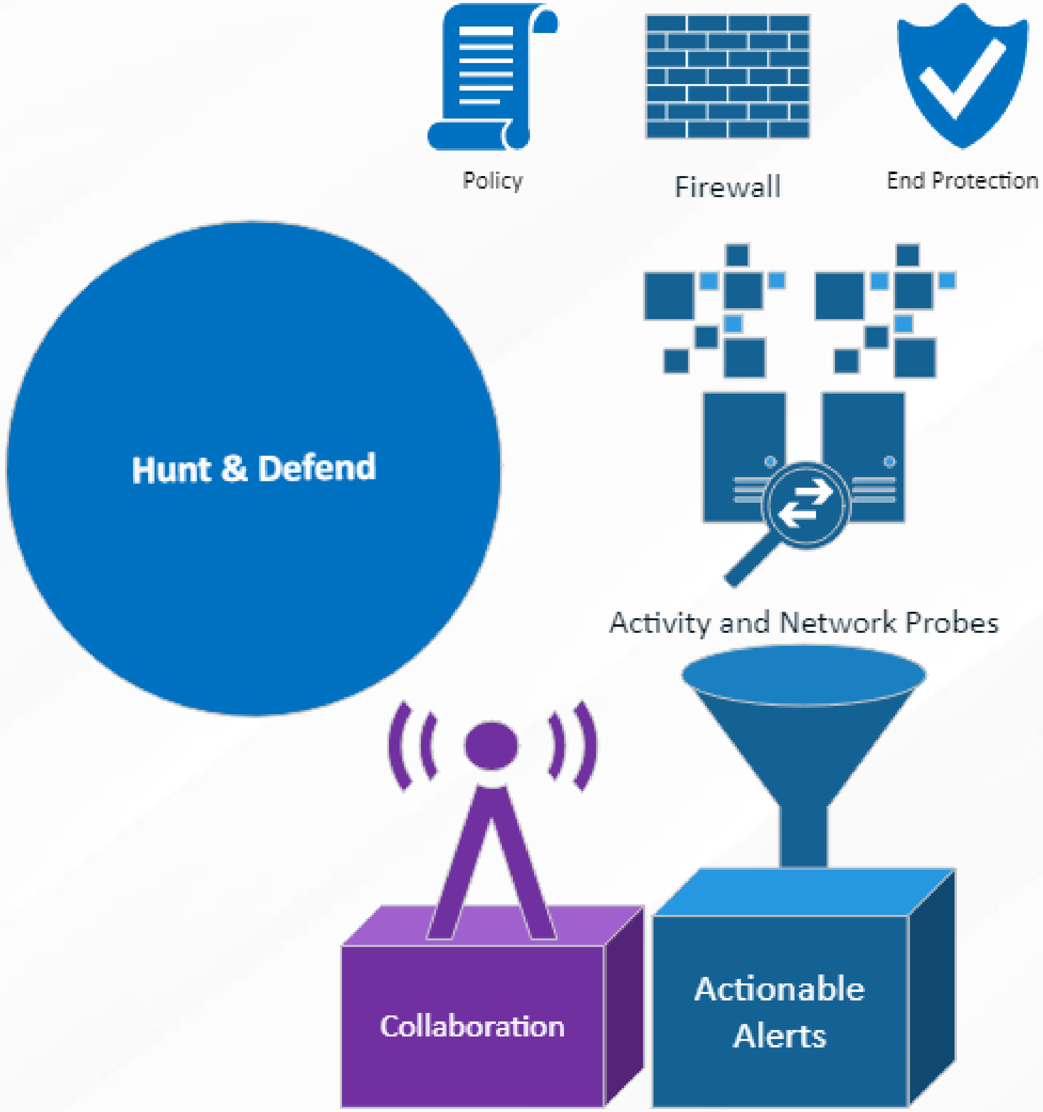
Goal: Find and Defend/Stop the Attack

How:

- Hunt Team Skills!
- Search Logs
- Review Endpoint Protection

Determine:

- New Tools Needed?
- Logs Need Adjusted?



ATOMIC PURPLE TEAM

5. Adjust & Harden

GOAL: Identify the changes necessary to be able to achieve the goals identified in planning.

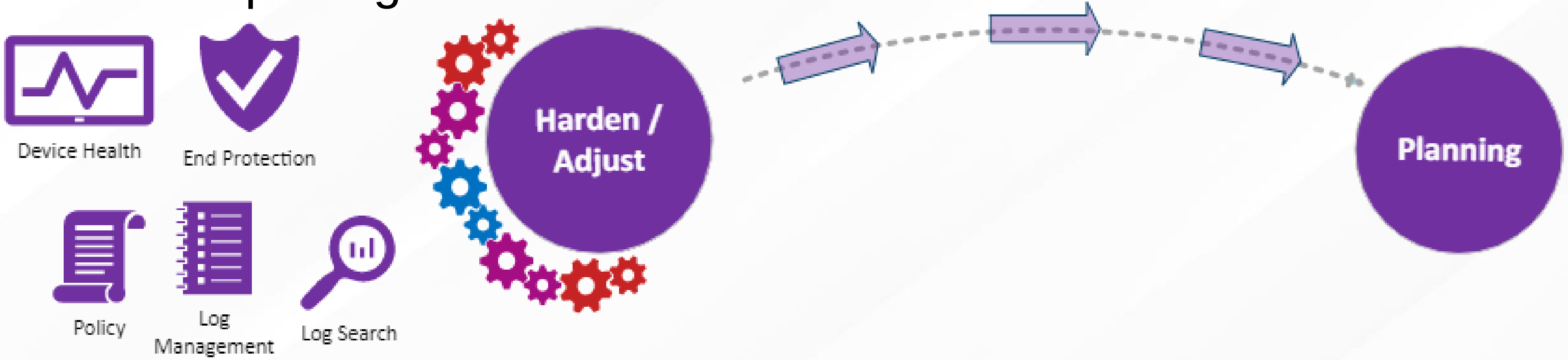
- Stop attacks / Identify Attacks / Alert

How: Modify policies, protections, logging to achieve goal.

- After changing, go to Planning phase and verify that you can achieve the goal (Stop/Identify/Alert)

Success: Move to Reporting Phase

ATOMIC PURPLE TEAM



Reporting and Request for Deployment

GOAL: Finalize the documentation of the Lifecycle engagement.

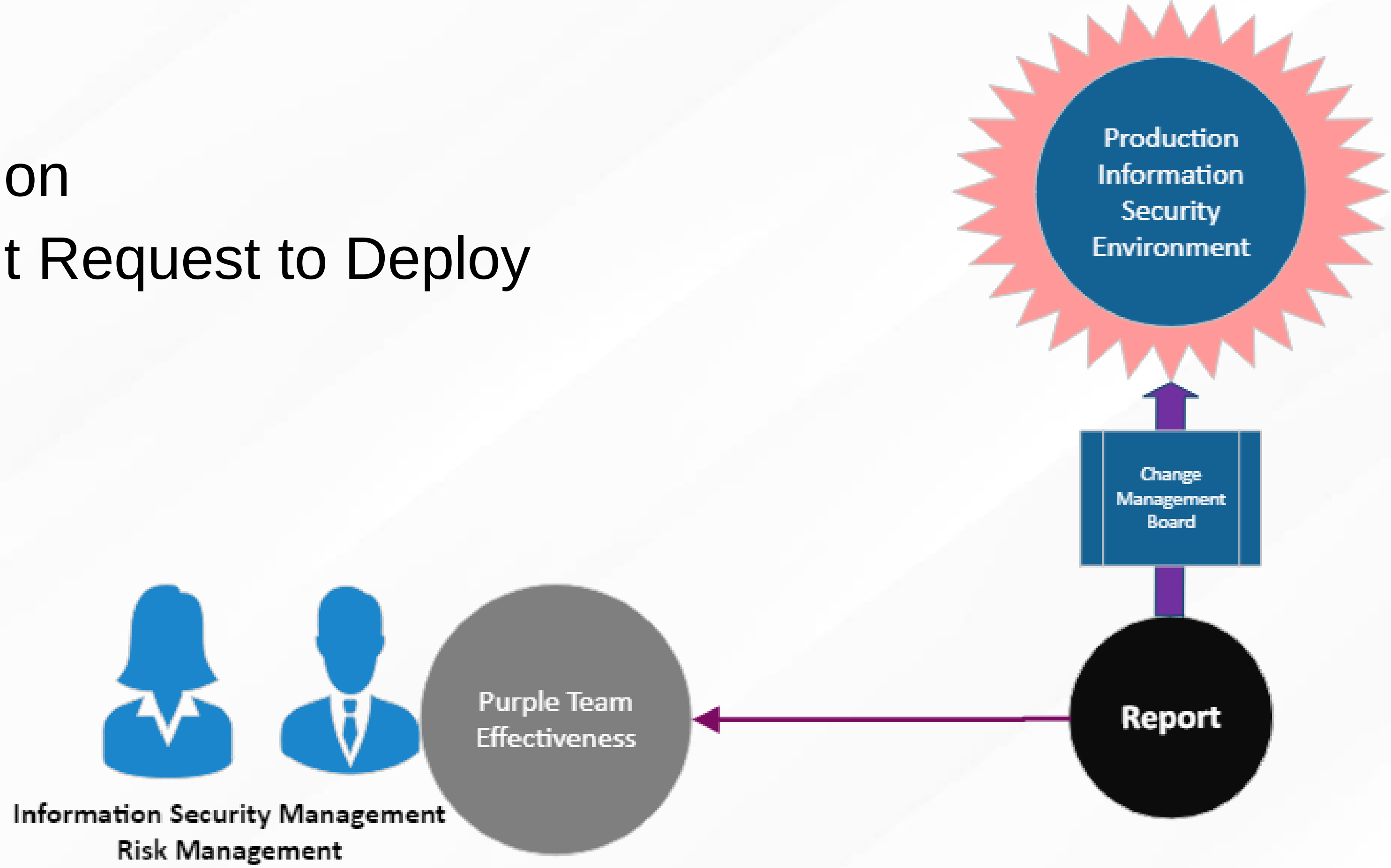
GOAL: With Success of the Lifecycle, Request deployment in Production.

How:

- Review Lifecycle Documentation
- Produce Change Management Request to Deploy

Done?

On to the next Lifecycle Rotation!


Production Information Security Environment
Change Management Board
Purple Team Effectiveness
Report
Information Security Management
Risk Management

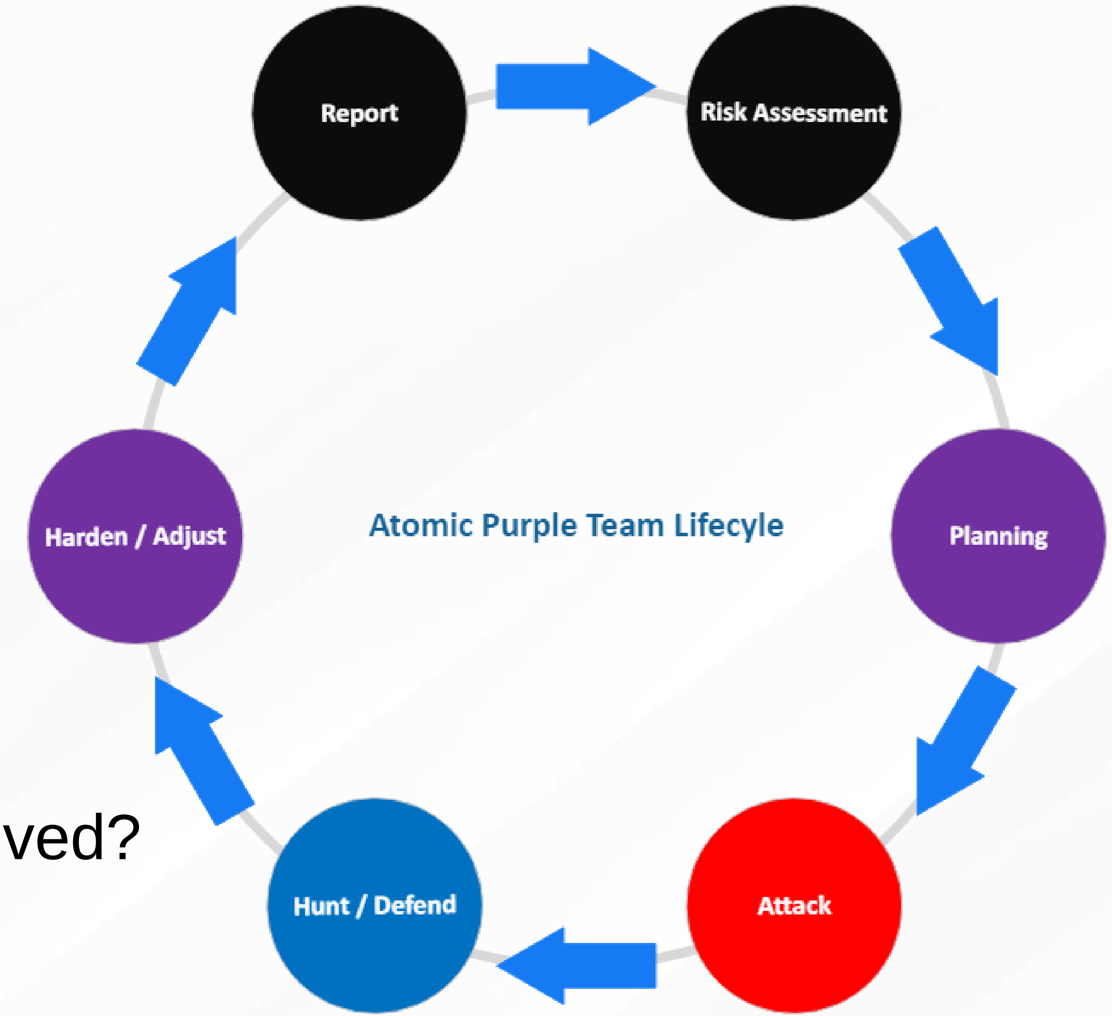
Lessons Learned

What can be done differently next time?

Were new techniques learned?

Do you feel you gained experience in "x"?

Has the organizations security posture improved?


Report
Risk Assessment
Planning
Attack
Hunt / Defend
Harden / Adjust
Atomic Purple Team Lifecyle