# MOBIA |

## *Adversary Simulation Workshop*

Spring 2021

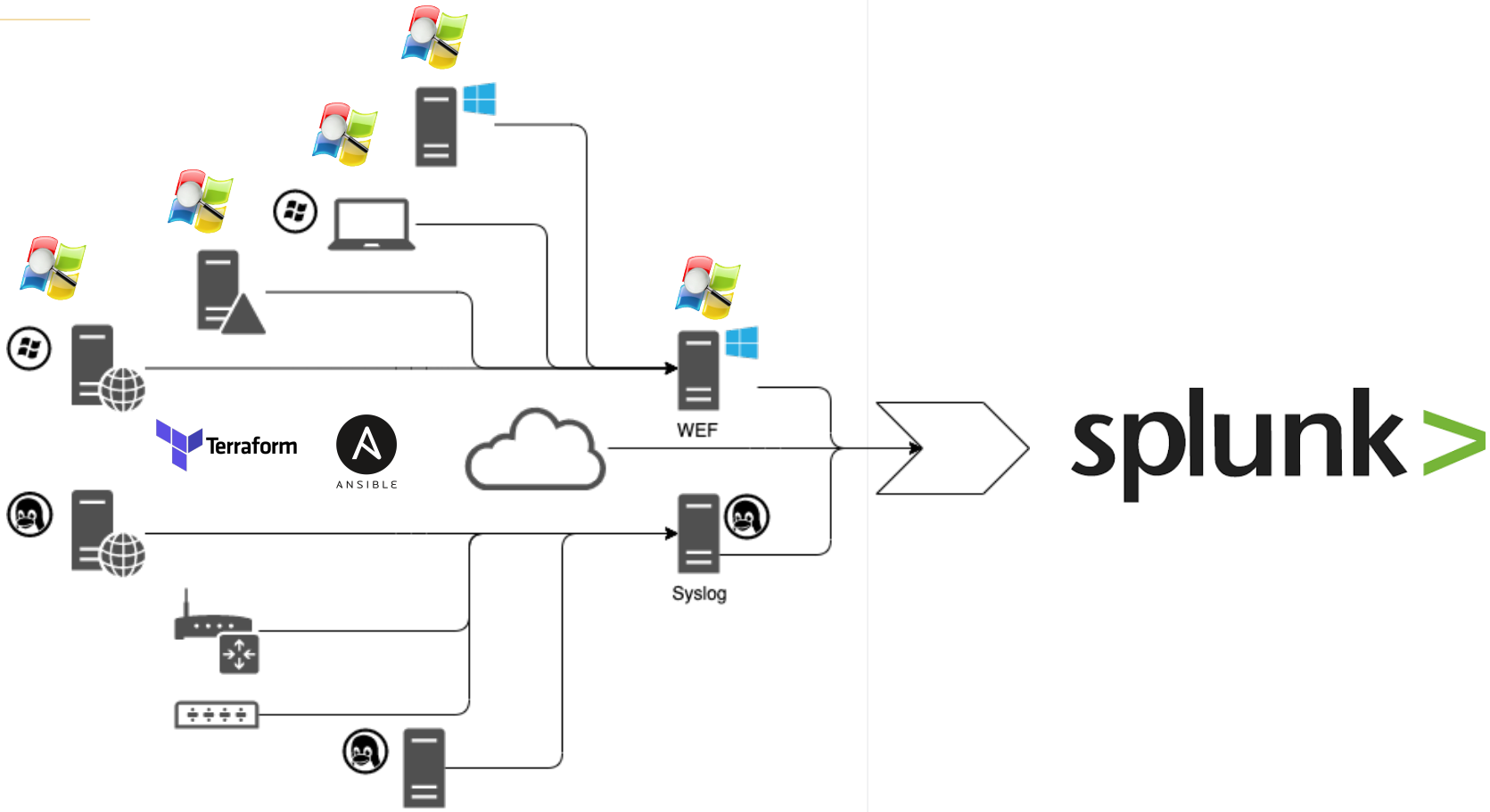
# Day 3:
# Events and Tracking

# Agenda

- Aggregating Events
- Mapping Detection Capabilities
- Building a Lab
- Labs!
- Building Repeatable Process
- Tracking Improvement
- Path to Continuous Assessment

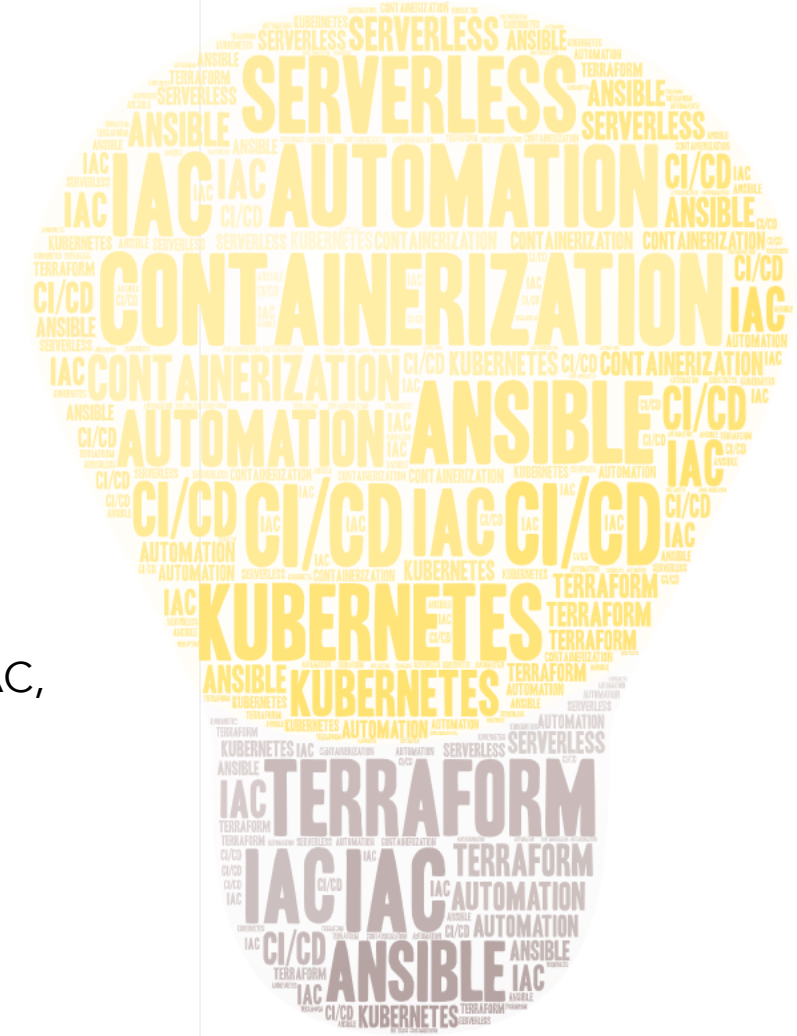
# Aggregating Events

- Ansible - Role for Splunk
- Olaf Hartong - Sysmon-modular
- Microsoft - Windows-Event-Forwarding
- Palantir - Windows-Event-Forwarding



# Aggregating Events

- Build Requirements
  - Infrastructure as Code (IaC)
  - Production-Like for Test
  - Low-Effort to Maintain
- SIEM Requirements
  - Handle dynamic data input (e.g. Syslog, JSON, Multiline)
  - Integrate well with other systems (e.g. Alert action, REST API, RBAC, Extensible)
  - Visualization
  - Performant on Scale
  - Join Disparate Sets of Data (Context)



# Mapping Detection Capabilities

- https://github.com/olafhartong/ThreatHunting
  Pre-built searches and Splunk app
- https://github.com/Neo23x0/sigma
  Vendor agnostic detection language
- https://github.com/rabobank-cdc/DeTTECT
  Map data sources to ATT&CK Navigator Layer
- https://github.com/olafhartong/ATTACKdatamap
  Map data sources to ATT&CK Navigator Layer

# Building a Lab

- https://github.com/clong/DetectionLab

  Building a production-like environment for testing

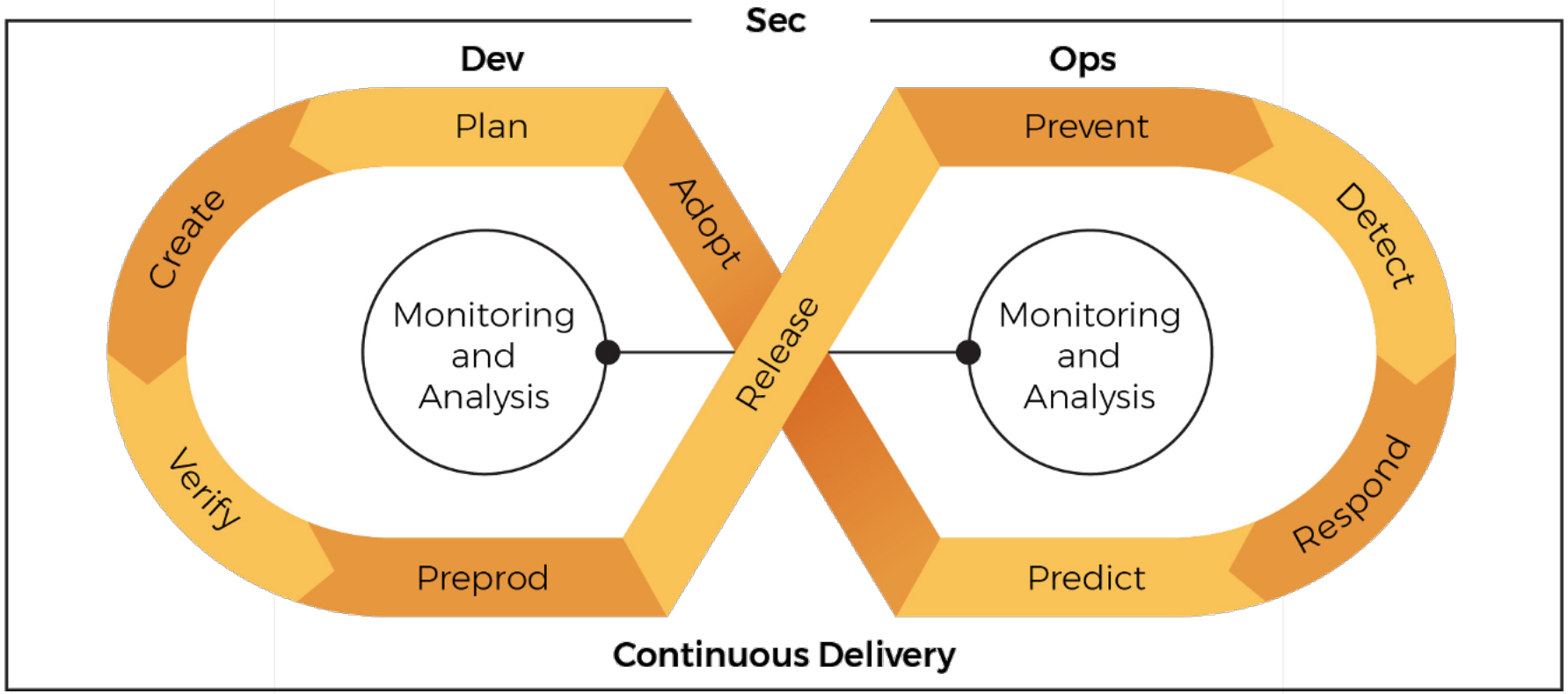
- https://github.com/splunk/attack_range

  Building a production-like environment for test

# LAB 11 – Login to Splunk (30 min)

# LAB 12 – ATT&CK Execution with Splunk (30 min)

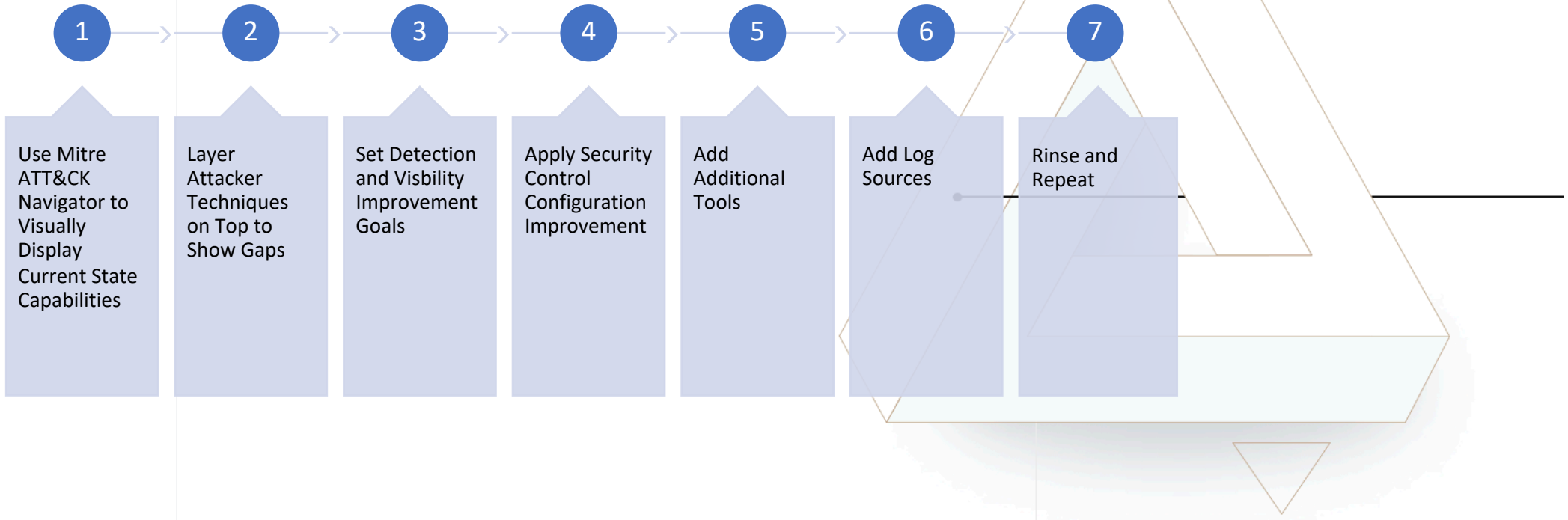
# Building Repeatable Process



# Building Repeatable Process

- PLAN
  - Gather attacker techniques
- CREATE
  - Develop test methods for attacker techniques
- VERIFY
  - Test current capabilities against attacker techniques
  - Prioritize gaps in protection and visibility based on current capabilities
  - Plan Changes in Security Tools Configuration and/or event Monitoring
  - Communicate current state and prioritized roadmap to senior leadership
  - Obtain budget for additional security tools and/or technical controls (optional)
- PREPROD
  - Update configuration of existing tools in production-like environment
  - Implement additional tools or technical controls in production-like environment (optional)
  - Test planned changes on production-like systems
- RELEASE
  - Update configuration of existing tools in production environment
  - Implement additional tools or technical controls in production environment
- PREVENT
  - Security controls provide protection against identified attacker techniques
- DETECT
  - Monitoring provides notification for operations when action is required
  - Anomaly detection provides insights into potential gaps
- RESPOND
  - Operations takes required action to investigate
  - Further action taken to mitigate damage as required
- PREDICT
  - Identify any additional gaps in protective controls
  - Better understand the mindset of your attacker and their methods
- ADOPT
  - Update current state and roadmap and reflect changes
  - Communicate current state and prioritized roadmap to senior leadership

# Tracking Improvement



# Path to Continuous Assessment

Establish security goals

Create an accurate picture of current security posture

Identify risks and vulnerabilities

Build a roadmap to continuous security assessment addressing identified risks and implementing new measures

Identify and propose solutions to enable continuous security assessment that are appropriate for your organization’s unique needs and goals

Guide and support the successful implementation of selected solutions

# Day 3 - Closing

- Aggregating Events
- Continuous Assessment
- Next Steps
- Thank you!