

# FloCon 2020

Using Data to Defend

JANUARY 6-9, 2020 | SAVANNAH, GEORGIA

## Methods for Testing and Qualifying Analytics

Timothy Shimeall, Ph.D.

CERT Situational Awareness Group

Software Engineering Institute  
Carnegie Mellon University  
Pittsburgh, PA 15213

The logo for FloCon 2020, featuring the text 'FloCon 2020' in a white, sans-serif font against a green background. The background of the entire slide is a dark green field with faint, glowing green and blue wavy lines, transitioning into a dark blue field with vibrant, multi-colored wavy lines on the right side.

# FloCon 2020

Using Data to Defend

JANUARY 6-9, 2020 | SAVANNAH, GEORGIA

## Methods for Testing and Qualifying Analytics

# Document Markings

Copyright 2019 Carnegie Mellon University.

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at [permission@sei.cmu.edu](mailto:permission@sei.cmu.edu).

CERT® and FloCon® are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM19-1255

# Overview

**Motivation and Definitions**

**Example Analytic**

**Test Framework**

**Qualifying Analytics**

# Motivation

It's only an analytic

- Just run it and see if it works
- It's only needed for this one incident
- It's too simple to worry about

I'm an analyst

- Not a developer
- Not a test/QA person
- Too busy for test

Takes too long to build (or fix)

Code starts generating poor results

- False positives / false negatives
- Too many resources needed
- Bugs / crashes / odd messages

Next person has to deal with it

- Poor idea what it does
- No clear flow of logic
- Mix of scripts/structures/languages

# Definitions

**Analytic:** A particular process that examines data to find trends and answer questions

- Descriptive analytics: find range and central tendency statistics on traffic
- Diagnostic analytics: track indicator that flags data exfiltration
- Predictive analytics: track indicator that suggests scanning prior to compromise
- Prescriptive analytics: flag traffic that is banned by policy

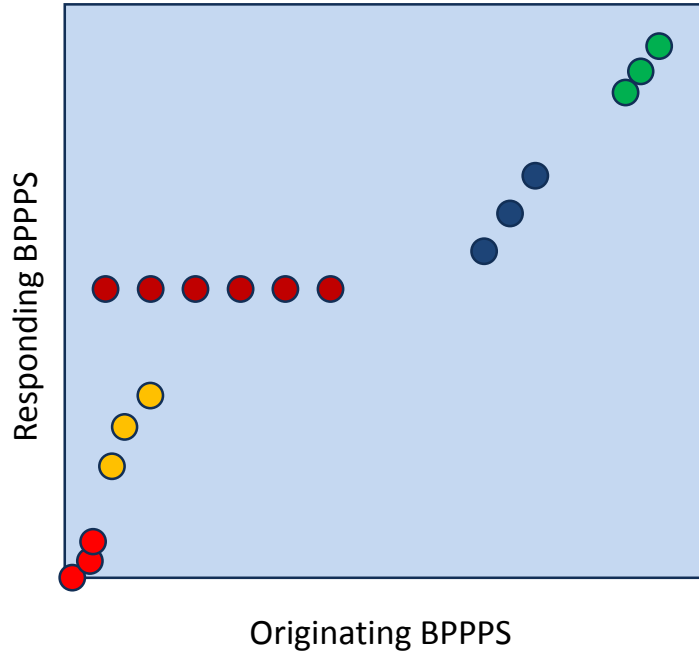
<https://www.mastersindatascience.org/resources/what-is-data-analytics/>

**Test:** A procedure intended to establish the quality, performance, or reliability of something, especially before it is taken into widespread use.

**Qualify:** Be entitled to a particular benefit or privilege by fulfilling a necessary condition.

<https://www.lexico.com/en/definition/test>

# BPPPS Analytic



Flow bytes per packet per second analytic

Mixing volumes and timing to separate:

- Signaling overhead (redundant close)
- Common attacks (brute force, port knocking)
- File transfer
- Interactive traffic

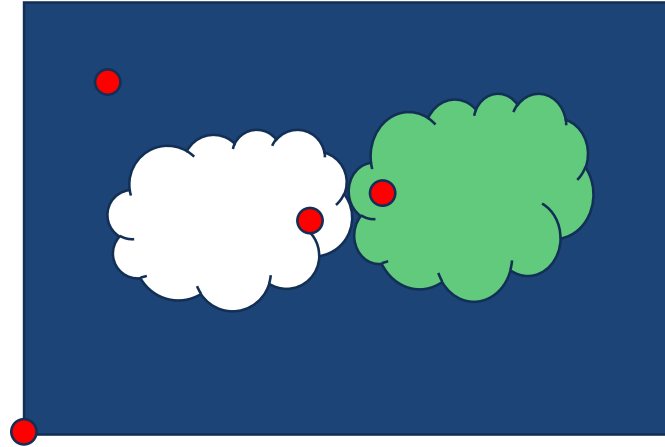
Port agnostic, not signature-based

# Test Design -1

## Data driven testing

- Normal input
- Null input
- Input for each output

## Output Space



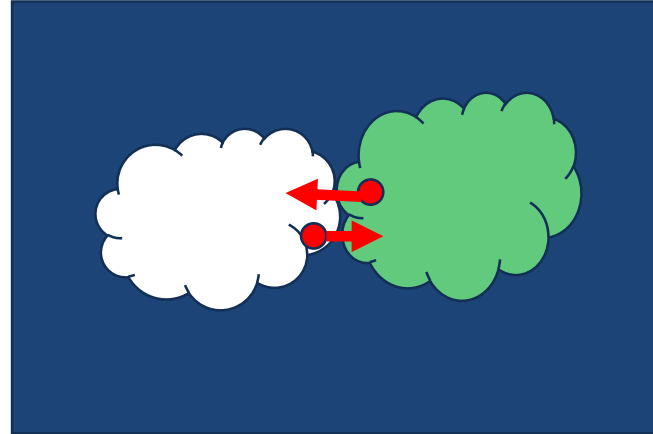


# Test Design - 2

## Case driven testing

- Where small addition changes output
- Where small deletion changes output
- Where reordering changes output

## Output Space

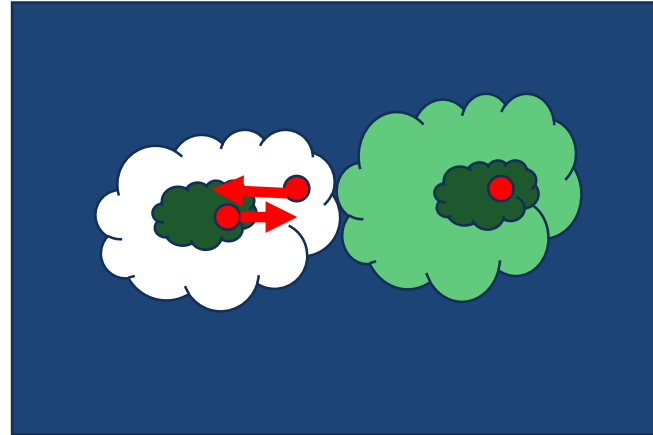


# Test Design – 3

## Threat Driven:

- Sample outputs associated with threats
- Where small addition can move non-threat to threat
- Where small deletion can move threat to non-threat

## Output Space

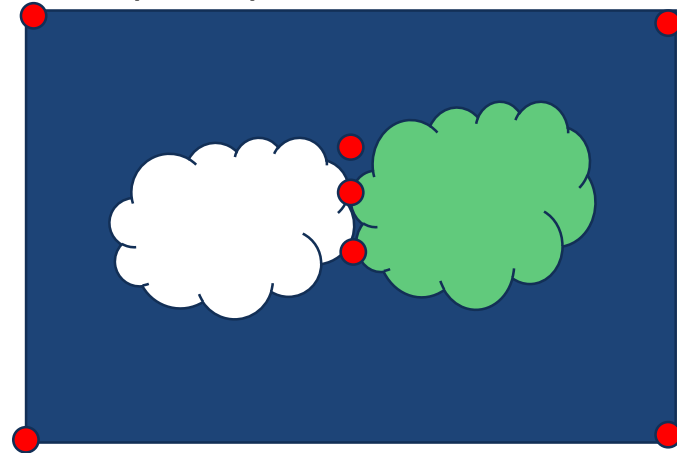


# Test Design - 4

## Bug-driven

- Where most likely omissions
- Where most likely confusions
- Where potential incompatibilities

## Output Space



# Qualifying Analytics

Reliability

Trust

Robustness

Maintainability

Compatibility

Security