MIS|TI™ PRESENTS

InfoSecWorld
Conference & Expo 2018

IMPACT OF SCALE ON SECURITY: AN OPEN DISCUSSION

Edward L. Haletky

Principal Analyst, TVP Strategy

Texiwill

ABSTRACT

Scale impacts security. As we scale up our environments, security gains more and more events, more and more things to look at. This roundtable seeks to develop actionable advice to cover these issues. Every aspect of security is on the table, so to speak.

We will discuss device authentication through application security, and everything in between. Is there one technology that provides an advantage? Is there one that does not work? This roundtable will seek to answer those questions while talking about strategy: The "how" and "why" of impact of scale into our environments. How do we address automation: is there a marriage between security and operations to consider, or is there another way to look at security?

TVP Strategy
Bringing Knowledge to In-KNOW-vation

InfoSecWorld
Conference & Expo 2018

DISCUSSION POINTS

Participants will discuss:

- What is Scale?
- Techniques to handle scaling up security
- Discover tools to help with scaling up security
- Convert specifics to generalized strategy for handling security at scale

WHAT IS SCALE?

- Scale seems to be different for everyone!

- Scale is?
  - Distances involved?
  - Volume/Velocity of requests, data, etc.
  - Number of devices, systems, etc. involved?
  - Something more than this?

HOW TO HANDLE SCALE?

How do we handle scale?

- Good planning
- Understand the control points. What are they?
  - How does this change with technology?
- Understand the technology. What are the limitations?
  - How does this change over time?
- Do the number of incidents go up over time?
- How does threat modeling fit into this?
- Examples anyone?

SOFTWARE DEFINED SECURITY?

- Software Defined Security?
- Is this the answer?
- What makes up software defined security?
  - Is it just automation?
  - Do we need a general model?
  - Is it just security as code?
  - Is there more to it?
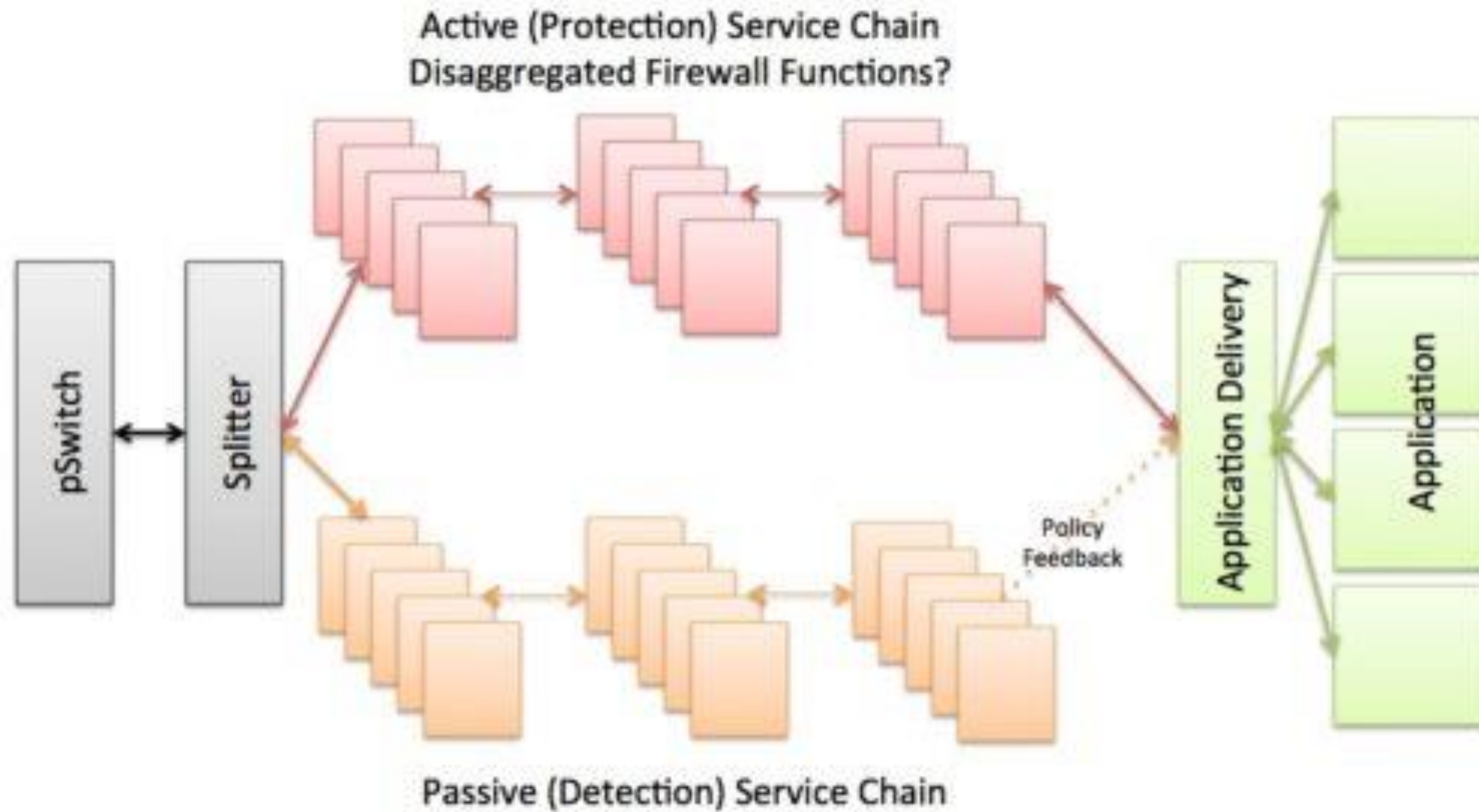
A MODEL FOR SECURITY AS CODE
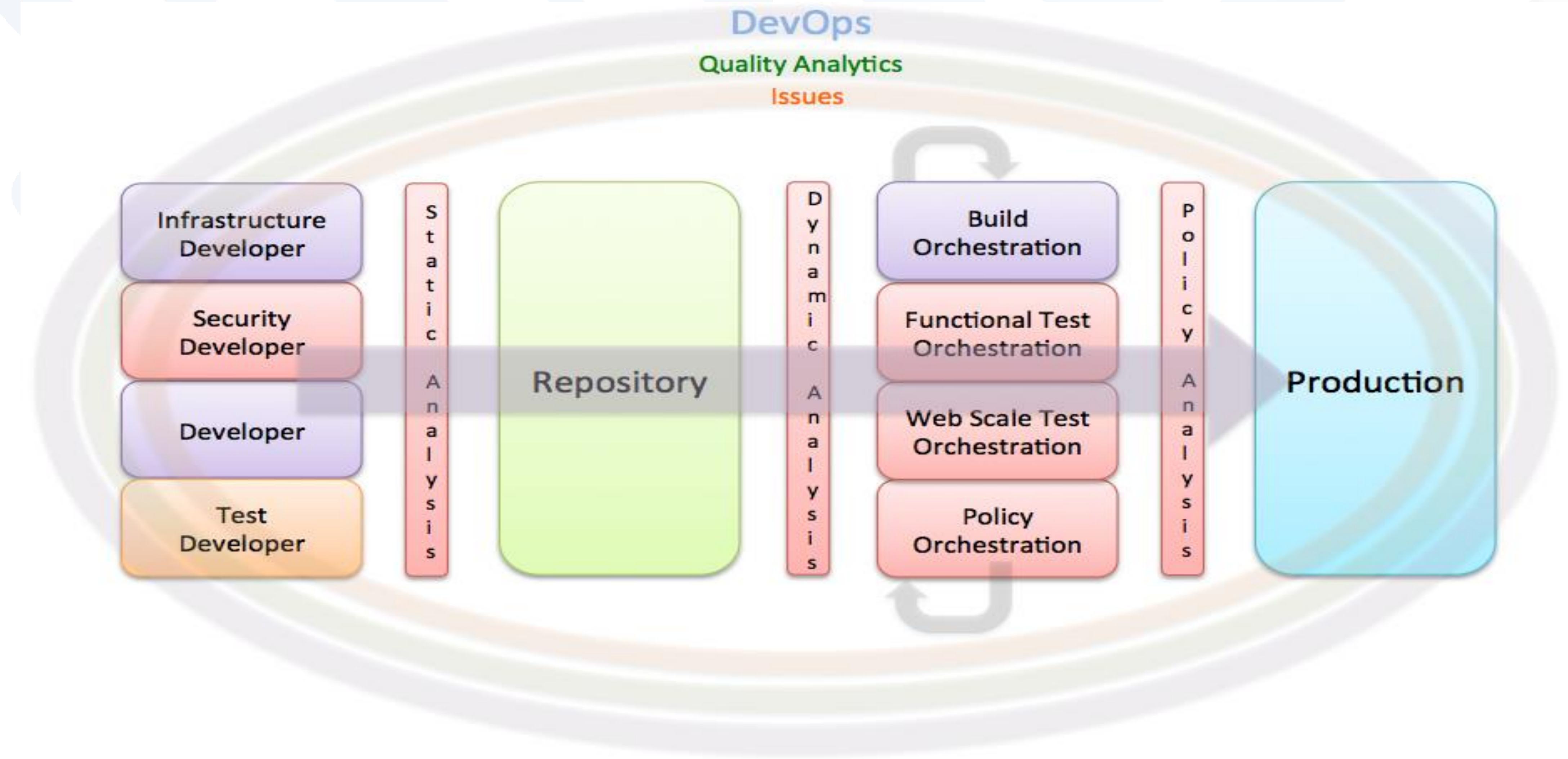
WHERE TO PLACE SECURITY?

Where do we place security?
- In front of the application?
- Beside the application?
- Within the application?
- Elsewhere?
- Does security need to be dis-aggregated?

APPLICATION?

Or do we move security into the application?
- Inside the code?
- A container around the code?
- A proxy in front of the service?
- Do applications change into a chain of micro-services?
- How do you reach scale?