UNC CHARLOTTE
College of Computing and Informatics

Defense Automation: SaltStack
in a Buzzword Rich Environment

Who am I?

- PhD Candidate at UNC Charlotte
- Director of Education for Ethical Hacking Club
- Defense Competition Enthusiast

Focus of Presentation

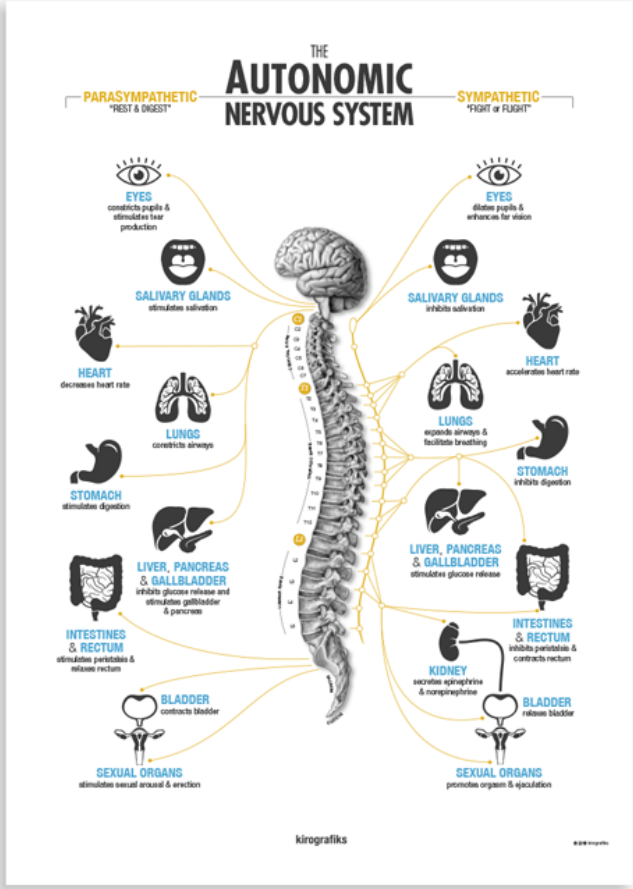
- Body of Research
- Applications of Autonomic Design
- Architecture and Scope
- Use of SaltStack
- Why Salt

Autonomic Computing

"… The obstacle is complexity. Dealing with it is the single most important challenge facing the IT industry.

- Paul Horn IBM "

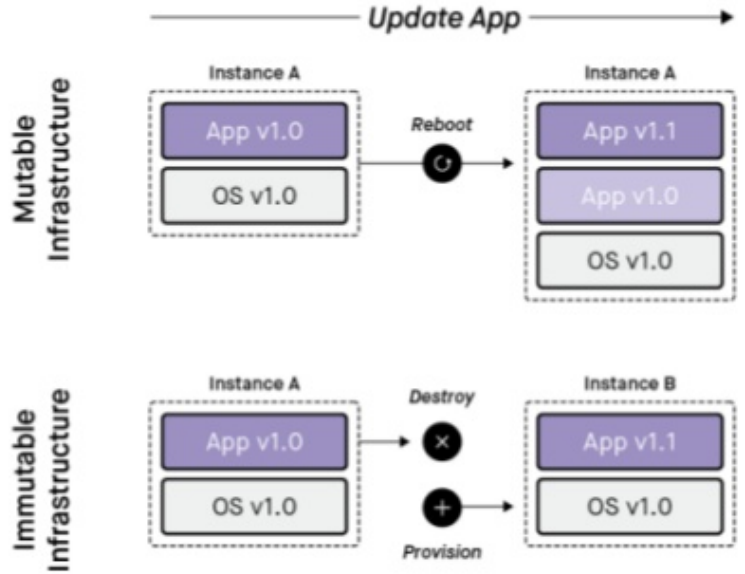
- Computer Immunology in 1998
- Autonomic Computing in 2001
- SARA (Architecture Reference) 2001
- Self-(x)



Components of Environment

- SDAR
- Infrastructure (D.I.E)
- Ability to Manage environment
- Ability to respond

Immutable Infrastructure

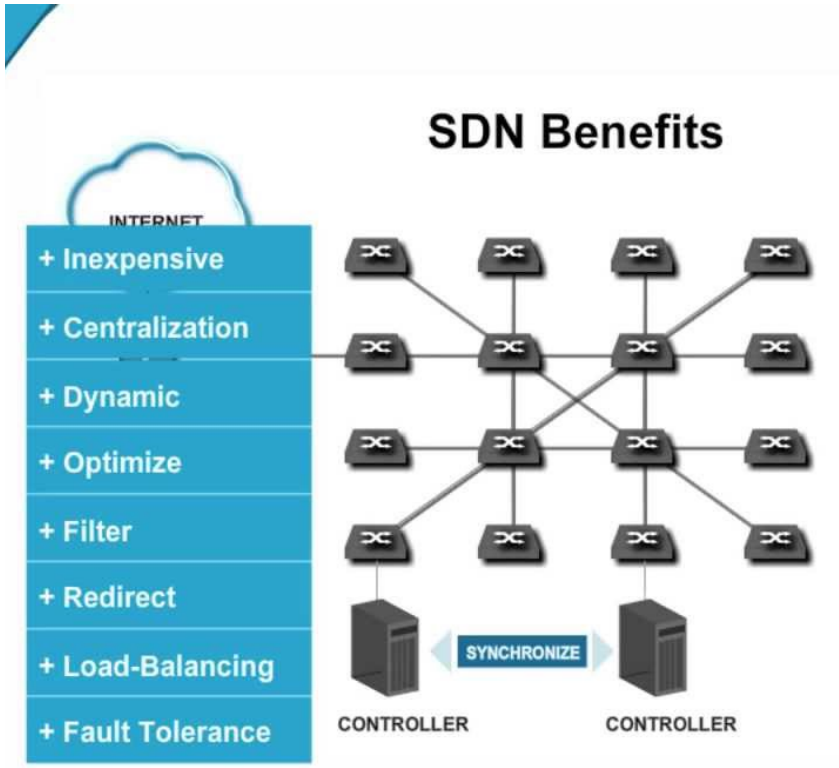


Josha Stella, *Immutable Infrastructure: Considerations for the Cloud and Distributed Systems*, 2016, O'Reilly
https://fugue.co/assets/docs/Immutable_Infrastructure_Fugue.pdf

Network Updates

How can we enforce distributed autonomic infrastructure?

- Software Defined Networking
- Dynamic routes
- Service redirection
  - *Inspiration from* HoneyMix

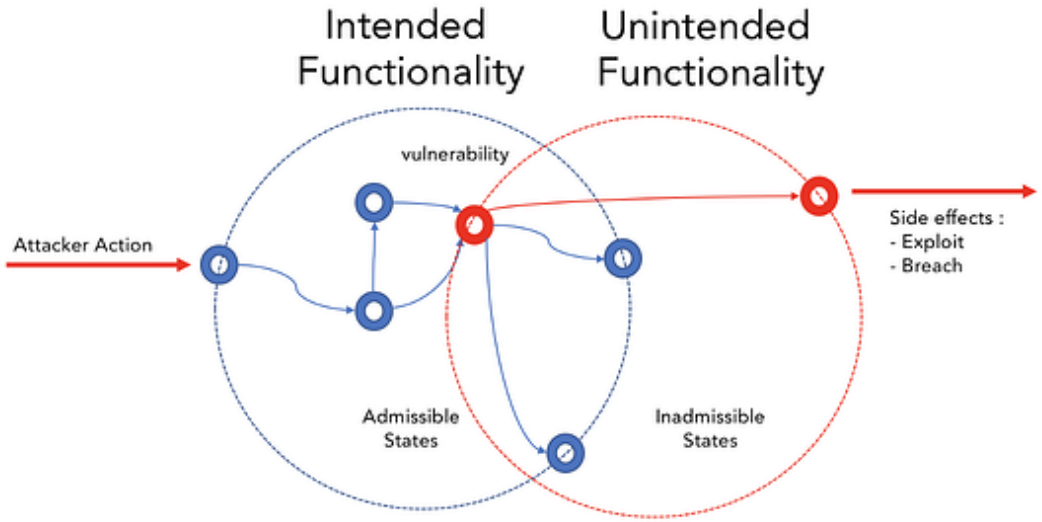


Orchestration

- Require Intelligent implementation
- Dynamic Policy enforcement
- Reduce reaction time

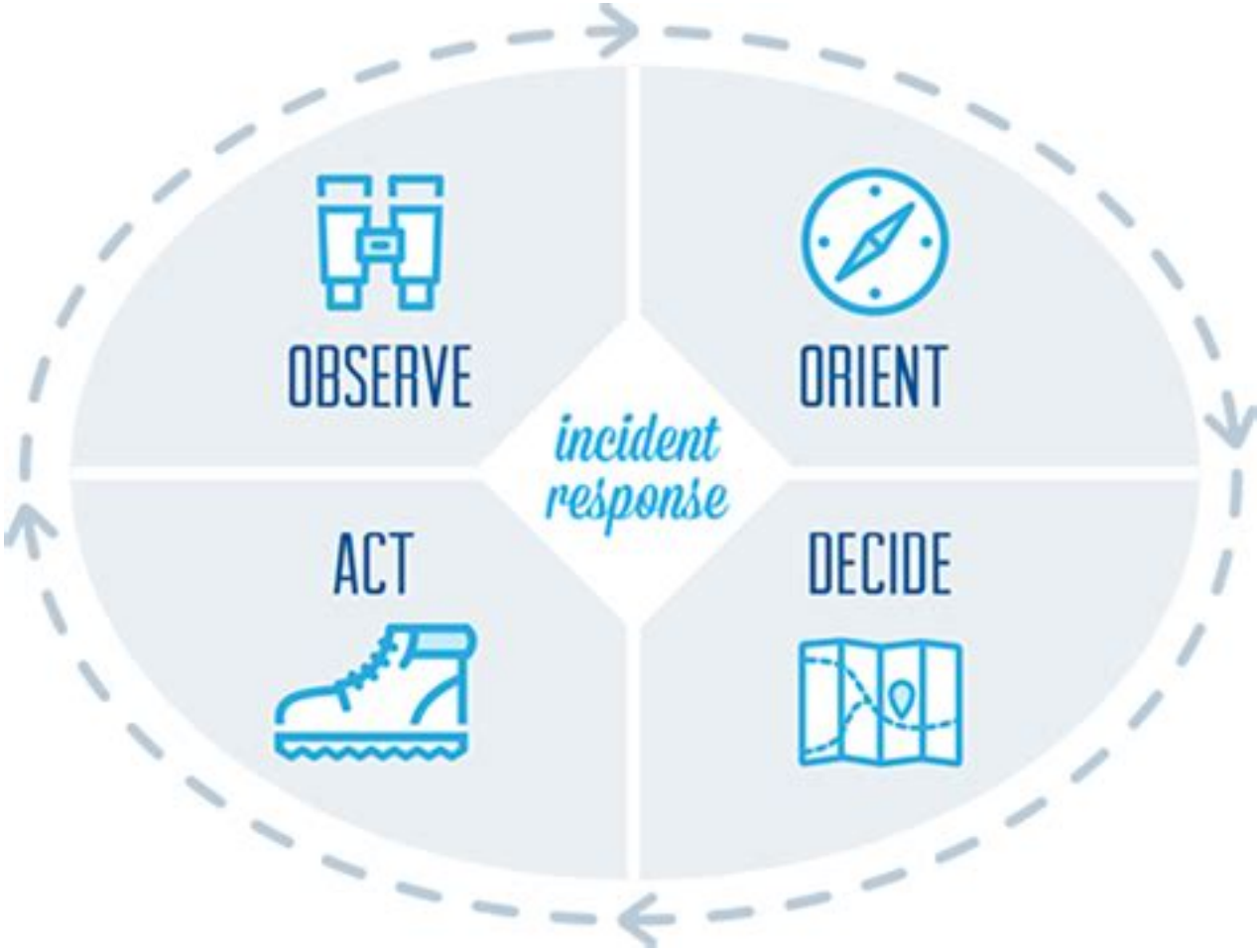
Feedback loops

- Optimizing Environment
  - Resource use
  - Snapshots
  - Load balancing
- Integrating learning into logic
  - How can Umbra help?



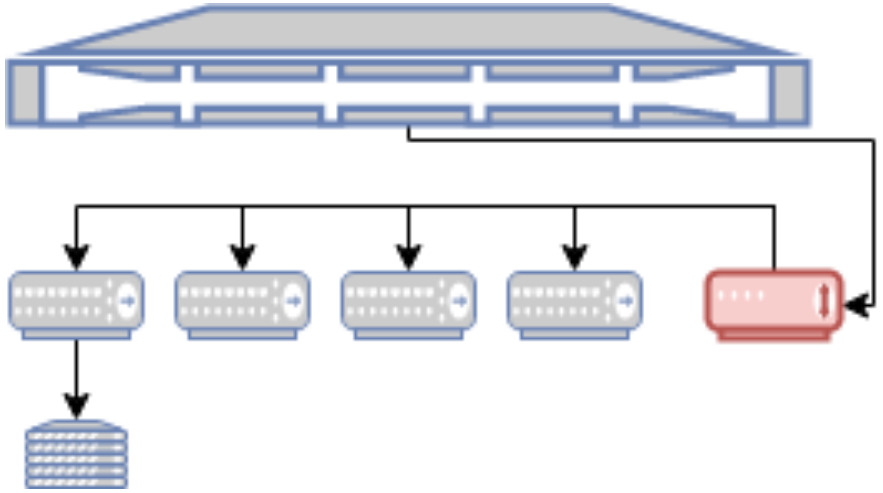
Optimal Goal

- Minimal down time
- Optimal response
- React at the time of detection



Implementation Overview

- Nested LXD Clusters
- SDN Container Networking
- Security Onion Integrations
- SaltStack Beacons and Reactors



Design Focus

- Updating network routes seamlessly
- Event response with Orchestration
- Ephemeral
- Feedback loops

Initial Impressions

- So many powerful components
- Event reactor and beacon system
- Integrating external tooling
- Enabling Security Onion Stack
  - Mike Reeves (2014)

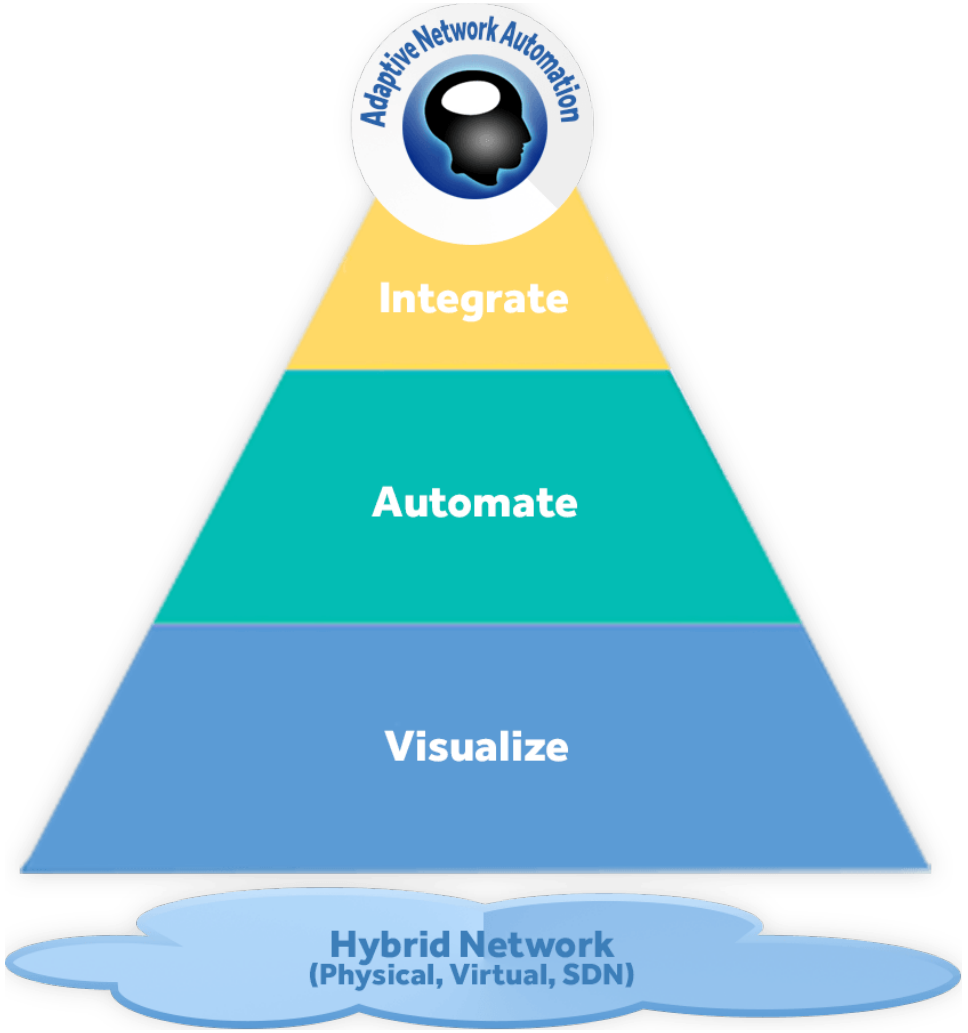
Insert tool trying to be SaltStack

Why SaltStack?

- Centralized/Decentralized
  - Multi-uses for master
- Uses python...
- Event Driven
- Extremely powerful for *free*

Using SaltStack

- Automating user polices
- Automating network policies
- Jinja
- Configured Beacon and Reactors

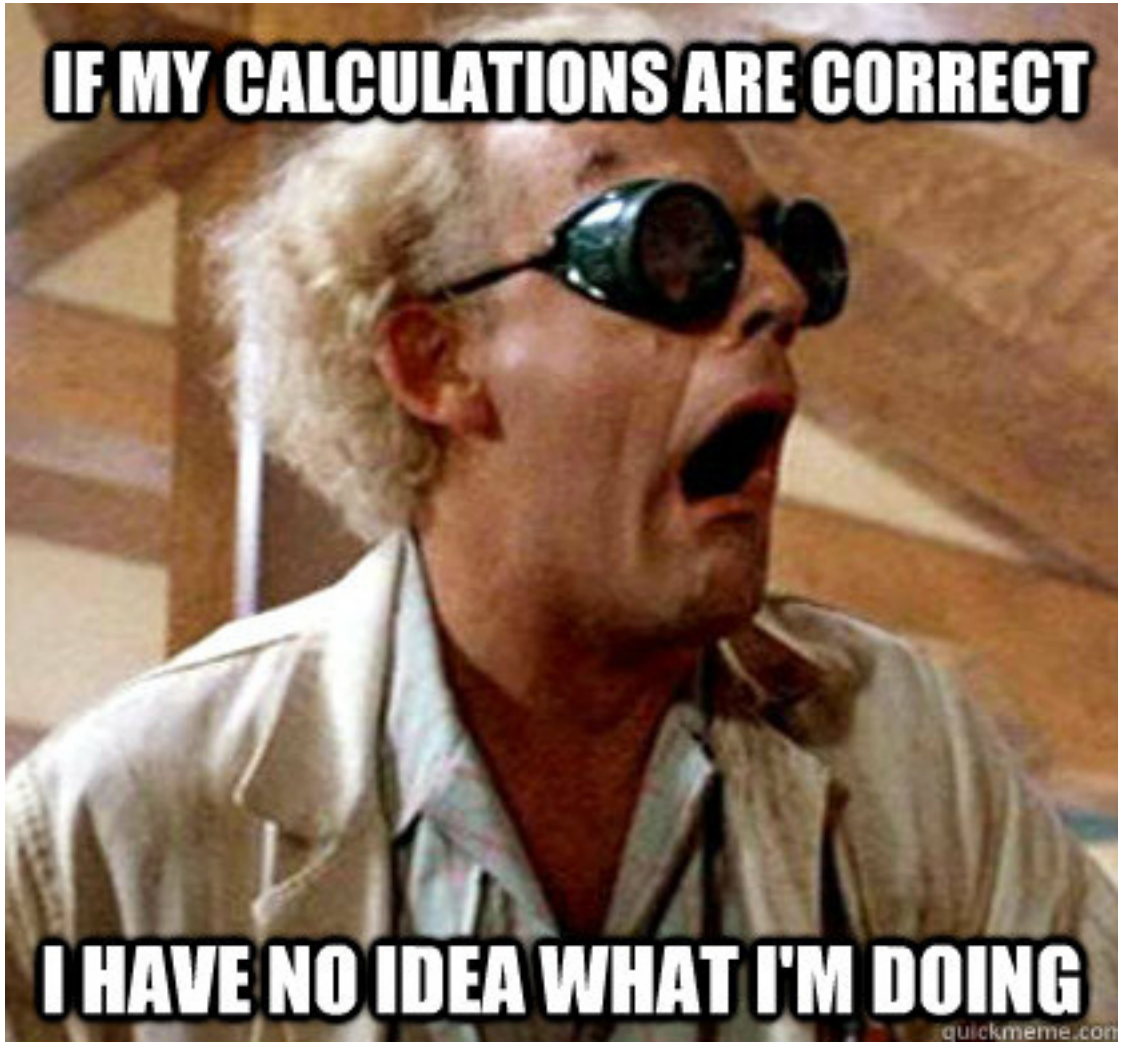


Challenges

- LXD Formula
- Making sure beacons work
- Network Automations
  - Network Function Virtualization

Closing Remarks

- Autonomic Computing
- SaltStack is enabling Autonomous System design
- POP, Umbra, and IDEM
- Code will be on GitHub soon…



Thanks for your time!

Connect with me…

- Twitter @trevonistrevon
- Website https://trevon.dev
- Keybase @blackmanta