The not so Ominous Future of Computer System Defense

Who am I

- PhD Candidate at UNC Charlotte
- Defense Competition Enthusiast
- 49sd Director of Education

Where are current advancements leading us?

Traditional System Defense

- SEIM
- [NG] Firewall
- Antivirus
- Alerting
- Threat Hunting

The Optimal Goal

- Respond at moment of detection
- Respond Optimally
- Increase cost of attacking network
- Secure all the things

Current Advancements

- Robust MTD (also via SDN)
- Active Cyber Defense
- Automated Network Management

How can we do better?

- Machine/Deep Learning
- The “Cloud”
- Blockchain
- Containers and Automation

So what if we put it all together?

**Excluding blockchain of course*

Disclaimer

This may not fit your business model

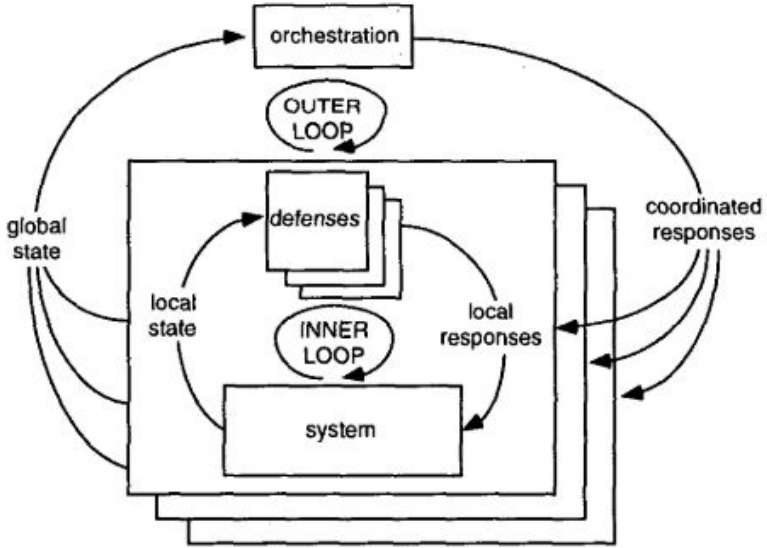
The *Bleeding* Edge

- Software Defined Networks
- SecOps/Automation
- Immutable Infrastructure… or not

Autonomic Systems

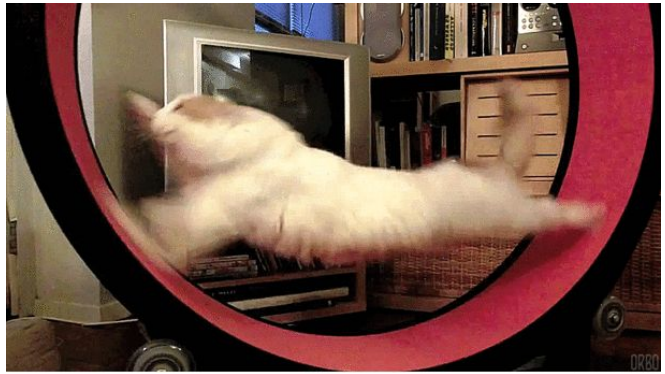
- Nervous System
- Self-(x)
- IBM and DARPA 2001
- IETF ANIMA

Components of an Autonomic System



Reactive Frameworks

- OODA (Observer, Orient, Decide, Act)
- MAPE (Monitor, Analyze, Plan, Execute)
- FOCALE (Foundation, Observe, Compare, Act, Learn, rEason)



Current Challenges

- Securing SDN
- Creating intelligent feedback loops
- Cool projects don’t last forever (runbook.io)
- Self-awareness systems

What does this mean?

In Summary

- Effective autonomic design is efficient and secure
- Autonomic features are here
- Reducing complexity at the cost of complexity

Thanks for your Attention

Twitter: @trevonistrevon

Website: trevon.dev

References

- D.I.E - Linkedin SlideShare
- DARPA SARA - Paper
- Network Fault Management - Paper
- RFC 7575 - Work group