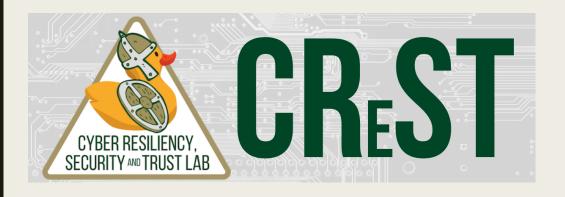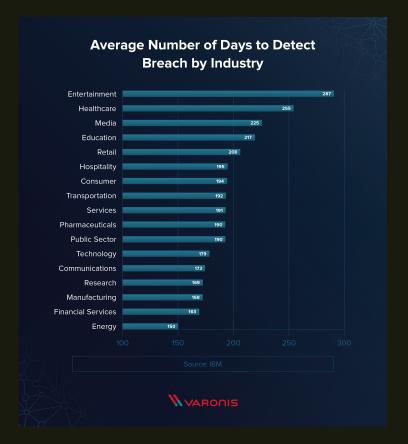# A *HACKERS* GUIDE TO CHEAP NGFW'S

Who am I

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

Area of Research

- Resilient and Autonomic Systems
- Agile network environments
- Software Defined Networks and Linux Containers

Average Number of Days to Detect Breach by Industry

Industry	Days
Entertainment	287
Healthcare	255
Media	225
Education	217
Retail	208
Hospitality	195
Consumer	194
Transportation	192
Services	191
Pharmaceuticals	190
Public Sector	190
Technology	179
Communications	173
Research	169
Manufacturing	168
Financial Services	163
Energy	150

Source: IBM

VARONIS

https://www.varonis.com/blog/data-breach-response-times/

Autonomic

- Self-*(x)
- Resilient by Default
- Automated Intelligence
- IT and Cybersecurity Oriented

NGFW

- Next generation firewall
- Policy Enforcement
- Sandboxing
- Intrusion Prevention

Traditional Firewall vs Next Generation Firewall

Software Defined Networking

https://www.youtube.com/watch?v=IPL_oQT9tmc

- Programmatically managing a network
- Powering the Cloud and Datacenters
- Southbound management
- Northbound integration

Demo

- Snort Integration with Controller
- Automating Sandboxing of Scan

NGFW

- Next generation firewall
- Policy Enforcement
- Sandboxing
- Intrusion Prevention

Traditional Firewall vs **Next Generation Firewall**

Traditional Firewall

Next Generation Firewall

Easier to Identify Threats

Application Based Filtering

Inspection of SSL/SSH traffic

Lower Administrative Cost

Identifying Network Traffic by User Groups

Better QoS

https://computersecuritypgp.blogspot.com/2016/04/next-generation-firewalls.html

Why is the important?

Takeaways

- Automation needs to intelligently built in

- Software defined networks

- Making tools work for you

Thank you

- @trevonistrevon (Twitter)
- https://trevon.dev
- https://github.com/trvon