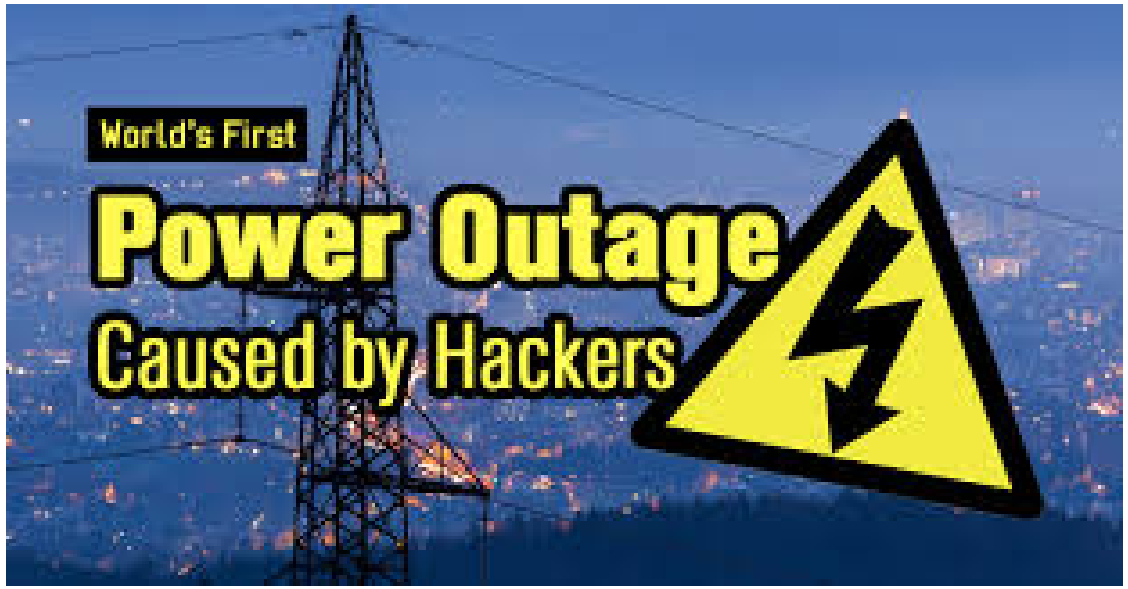
TRAIN LIKE YOU FIGHT

MODELLING CYBER REAL-WORLD SCENARIOS

Alexandru Enache, System Engineer

UKRAINE ELECTRIC GRID HACK



- Phishing Email
- 'KillDisk' and BlackEnergy 3
- Coordinated DDoS attack

- 23rd of December, when half of the staff is off duty

http://thehackernews.com/2016/01/Ukraine-power-system-hacked.html

ixia

Current Defense Mechanisms and Challenges

Cyber Defense Technologies

- ✓ Network Based Mitigation
  - Applications awareness and control
  - User Identity and Control
  - Content Security (IPS, GAV, DLP, AntiSpam)
  - SSL encryption/decryption
  - DDoS mitigation
  - IP reputation, URL filtering
- ✓ Network Behavior Analysis Detection
  - collects and analyzes traffic from the entire network — host and applications
- ✓ Host Based Mitigation (AV, DLP, IPS)
- ✓ Vulnerability Management

Cyber Defense Challenges

- ✓ Cyber Security Threats have become more complex, targeted and persistent
- ✓ The Information Security landscape is constantly evolving
- ✓ Borderless Networks
  - driven by new technologies and trends (Mobility/BYOD, Cloud, Social Media)
- ✓ Staff Education
  - How to test and train with network and Internet technologies and systems

ixia

Modern cyber-defenses require proactive security operations

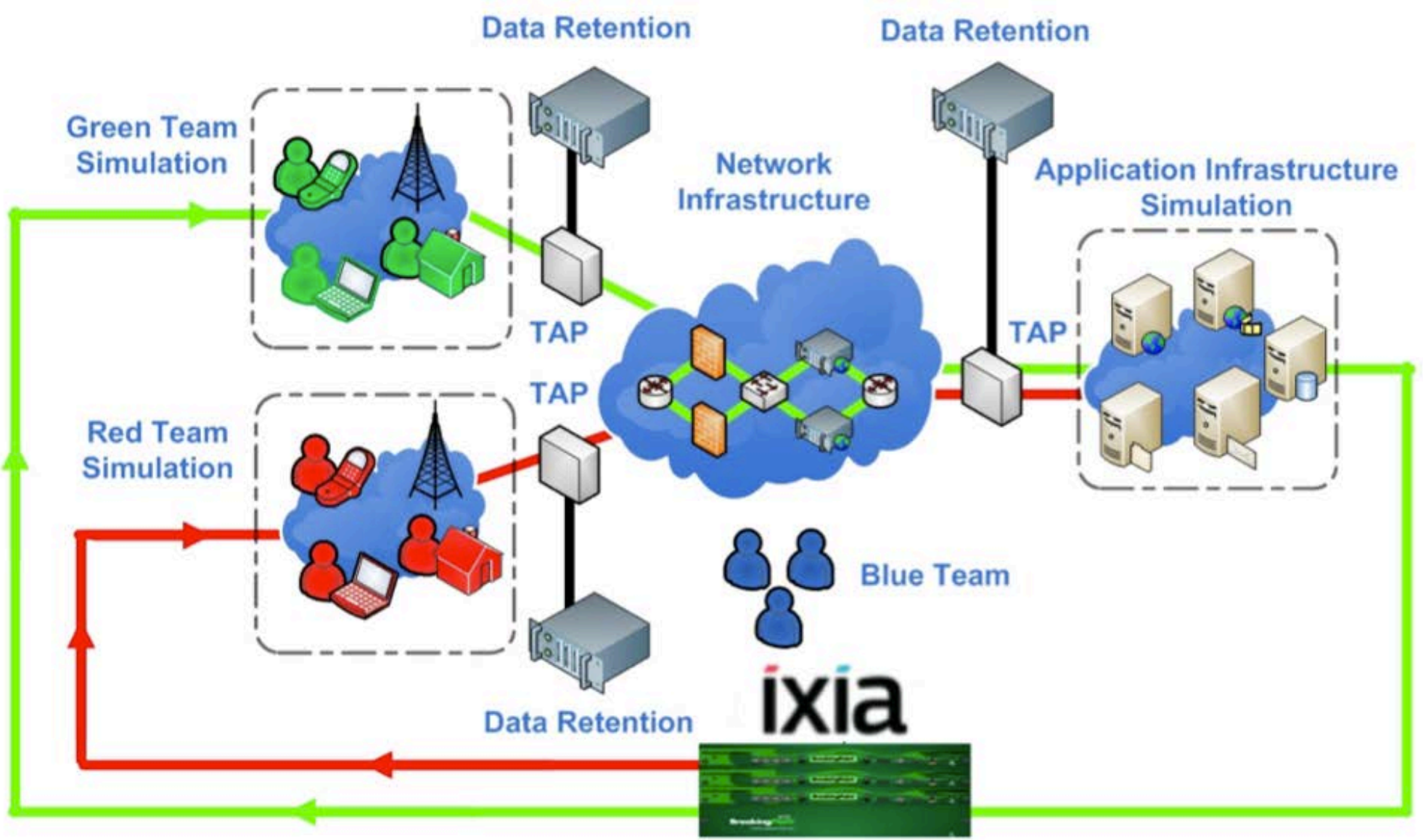
Cyber ranges help security staff build the skills and experience necessary to combat modern cyber threats

TRAIN LIKE YOU FIGHT!

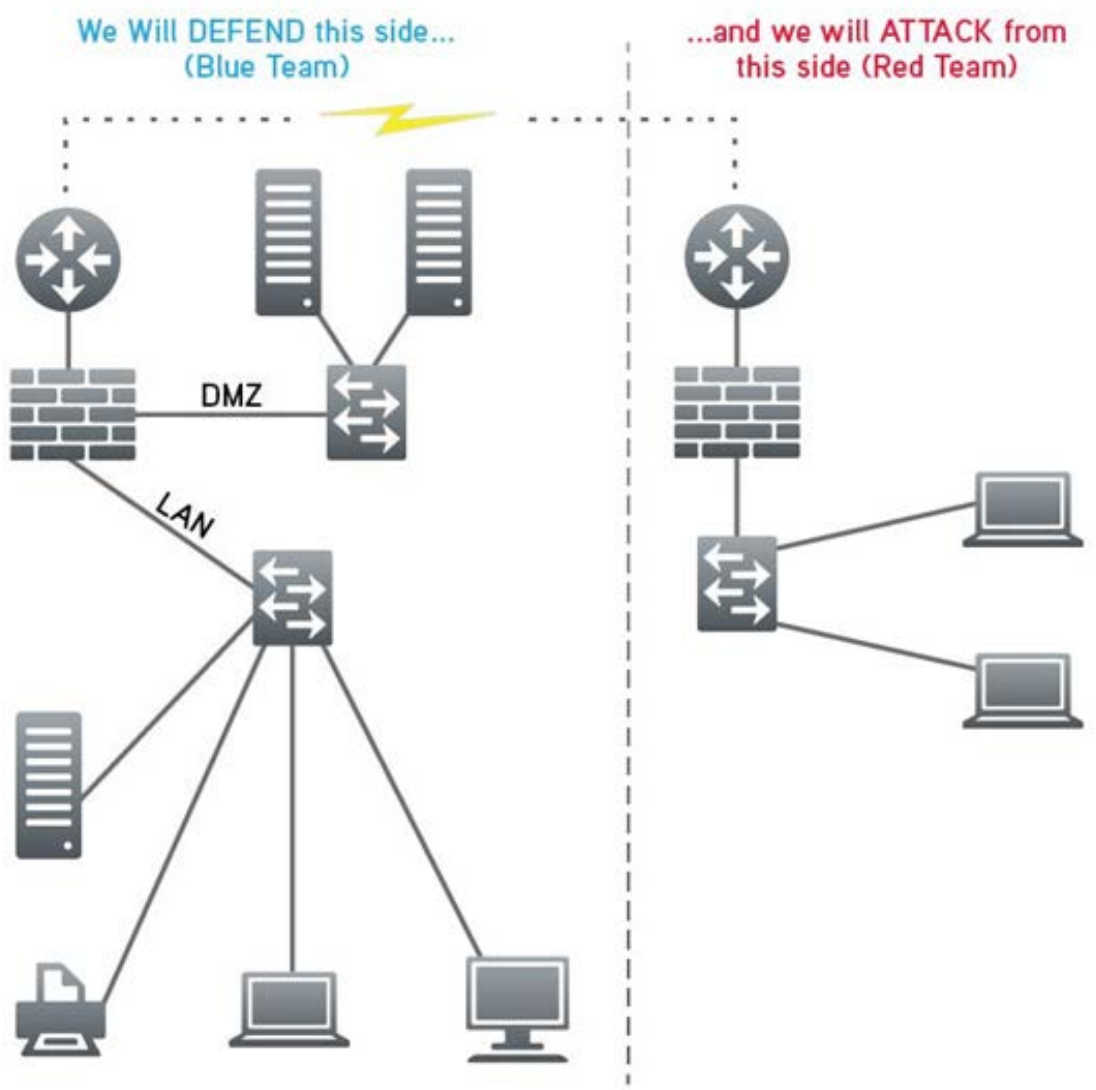
- No more “hearers and seers” protecting our networks and critical infrastructures
- How do we manage in a complex and ever changing environment?
- Education and Training Afforded by Realistic Cyber Ranges Can Stem the Gap

5

CYBER RANGE INTEGRATION



CYBER RANGE ENVIRONMENTS



Physical / Virtual / Hybrid Cyber Range

- Physical Cyber Range: Very realistic but has a huge financial cost and long time to set up.
- Virtual Cyber Range: Low cost, but limited in emulating full performance of security devices
- Hybrid Cyber Range: Balanced approach. Combine flexibility with performance

THE KEY IS REALISM

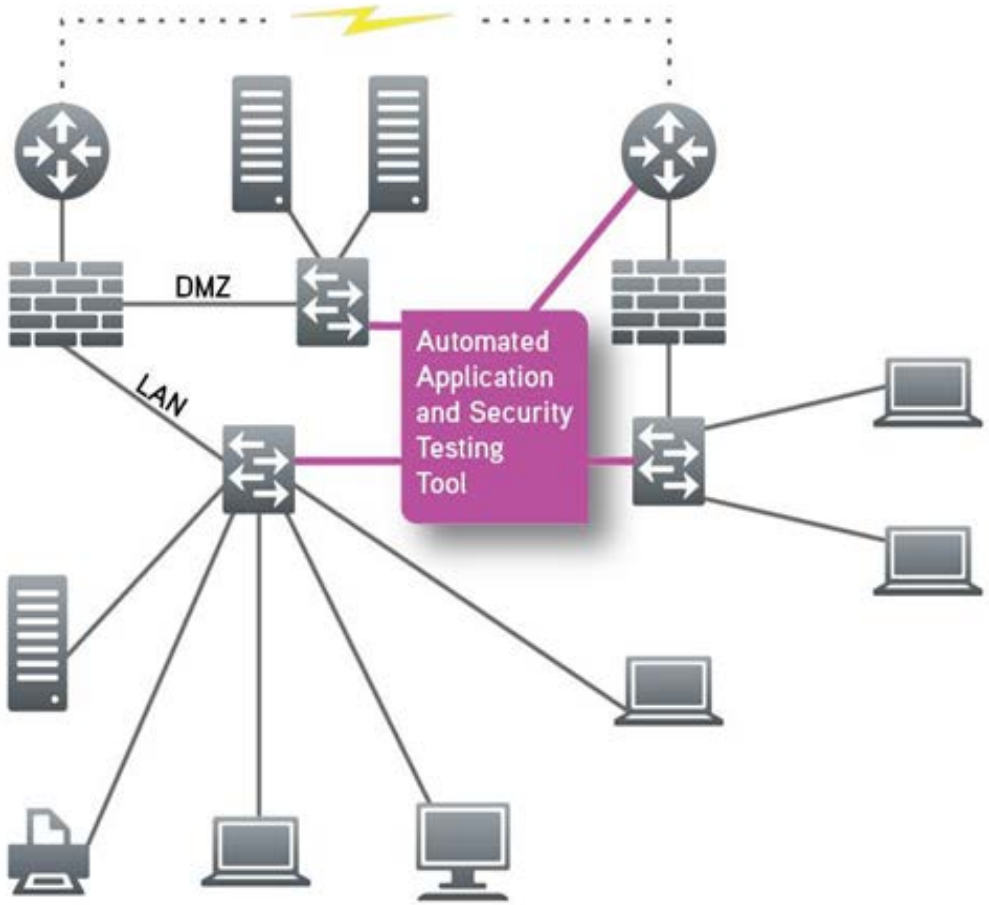
- How do you manage realism?

- To encourage realism, your range configuration will have many critical considerations
  - Human capital
  - Different attack/defense paradigms
  - Scale

- Many challenges
  - How do you model tens, hundreds, thousands, or more employees and the constantly changing applications and data they use on a day to day basis
  - How to gain expertise to generate effective attack scenarios to stress network defenses in your range (internal personnel, outside resources, etc.)
  - How do you scale those attack vectors when you don't have the computing resources of a worldwide botnet at your disposal?

8

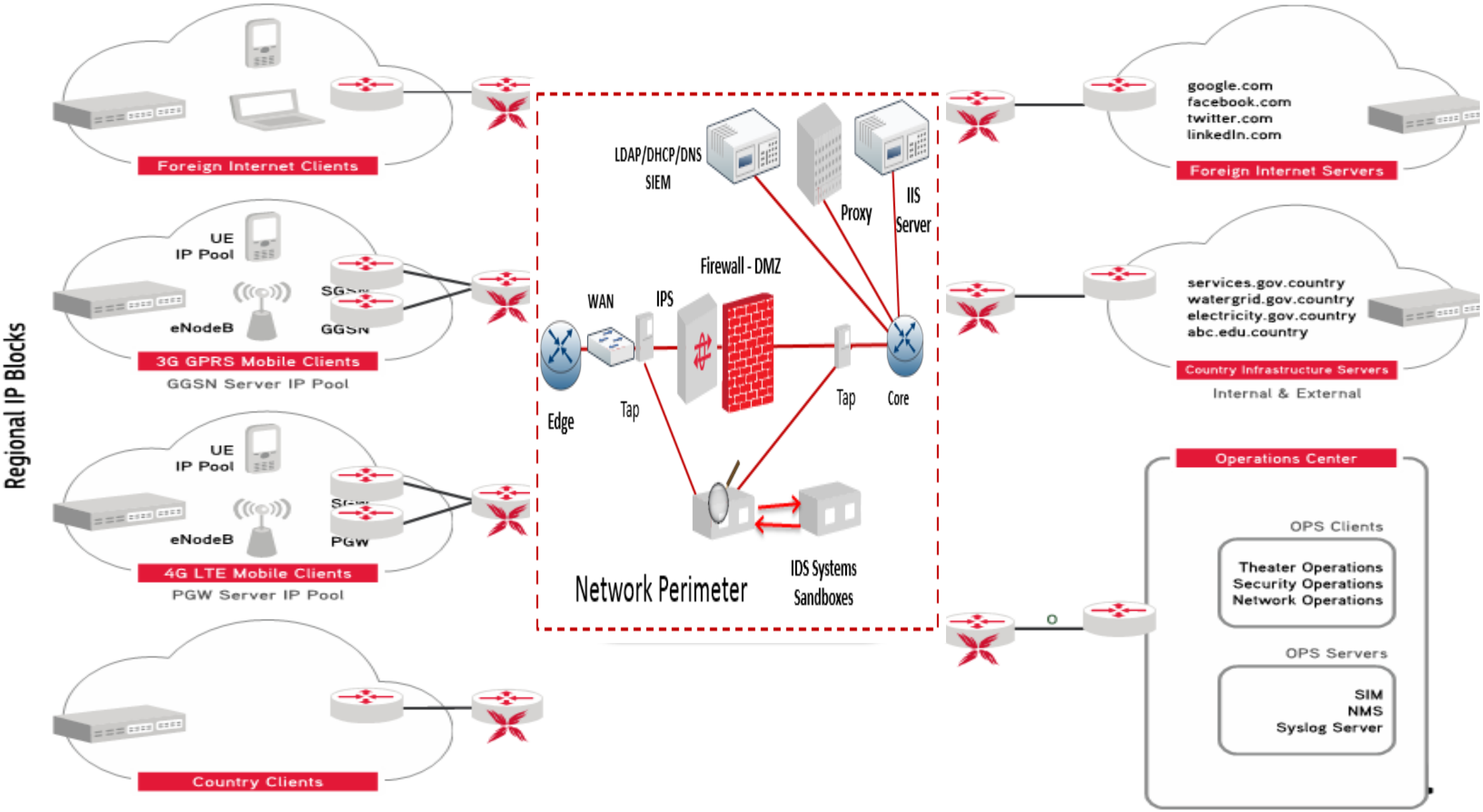
CREATING AND MANAGING REALISM – TRAIN LIKE YOU FIGHT!



- Employ actual people on the range – doesn't scale to more than a few people
- Capture and replay production network traffic – don't allow for real world data randomness over time
- Use a set of automated tools to quickly and efficiently pick and choose what you want your background traffic mixes and attack traffic mixes to look like
- **Or you could do the smart thing, and use a hybrid approach of all of these, and in doing so, create the Next Generation Cyber Range**

ixia

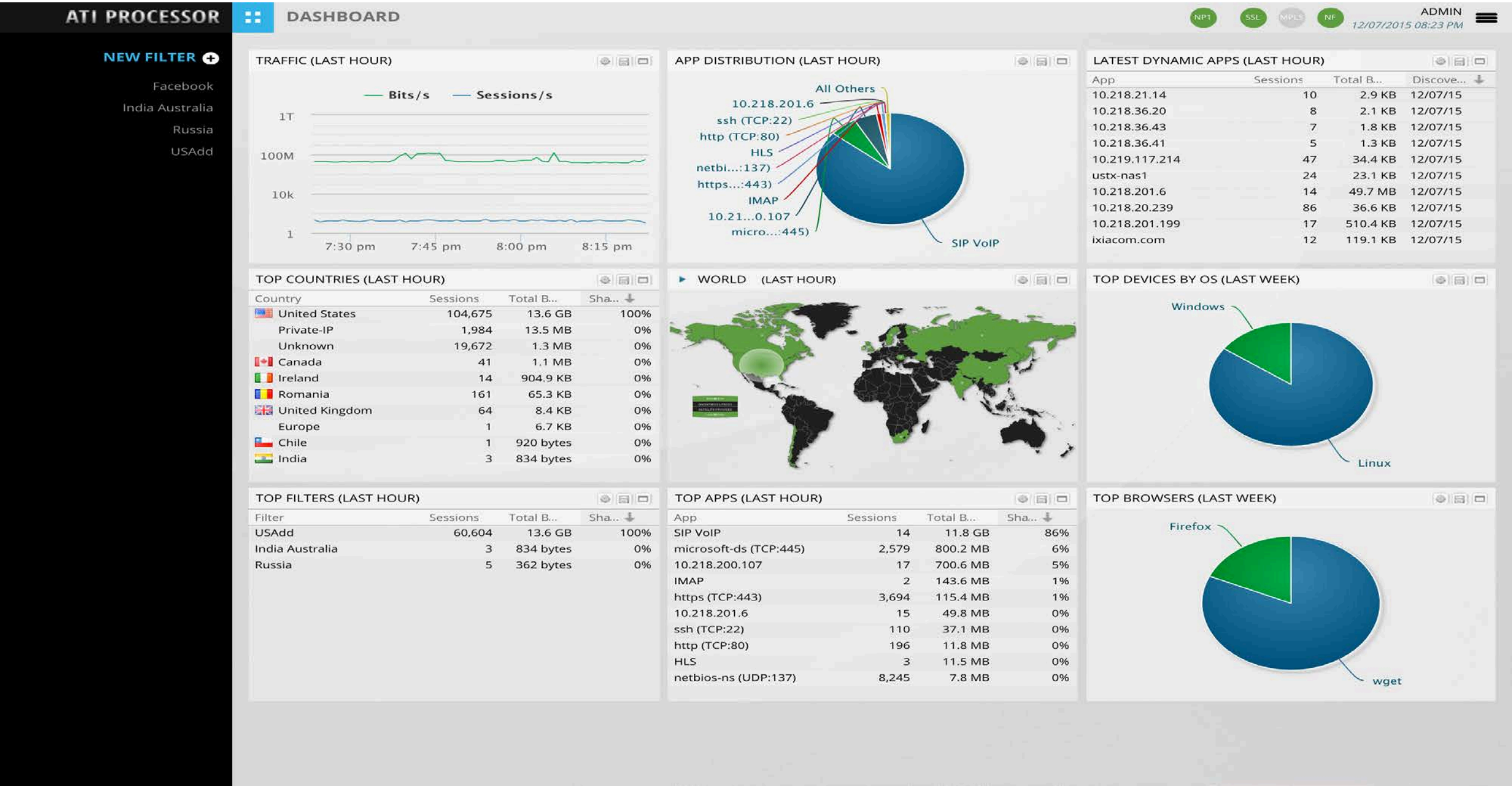
HIGH LEVEL TOPOLOGY



BLUE TEAM – SIX STEPS OF INCIDENT RESPONSE

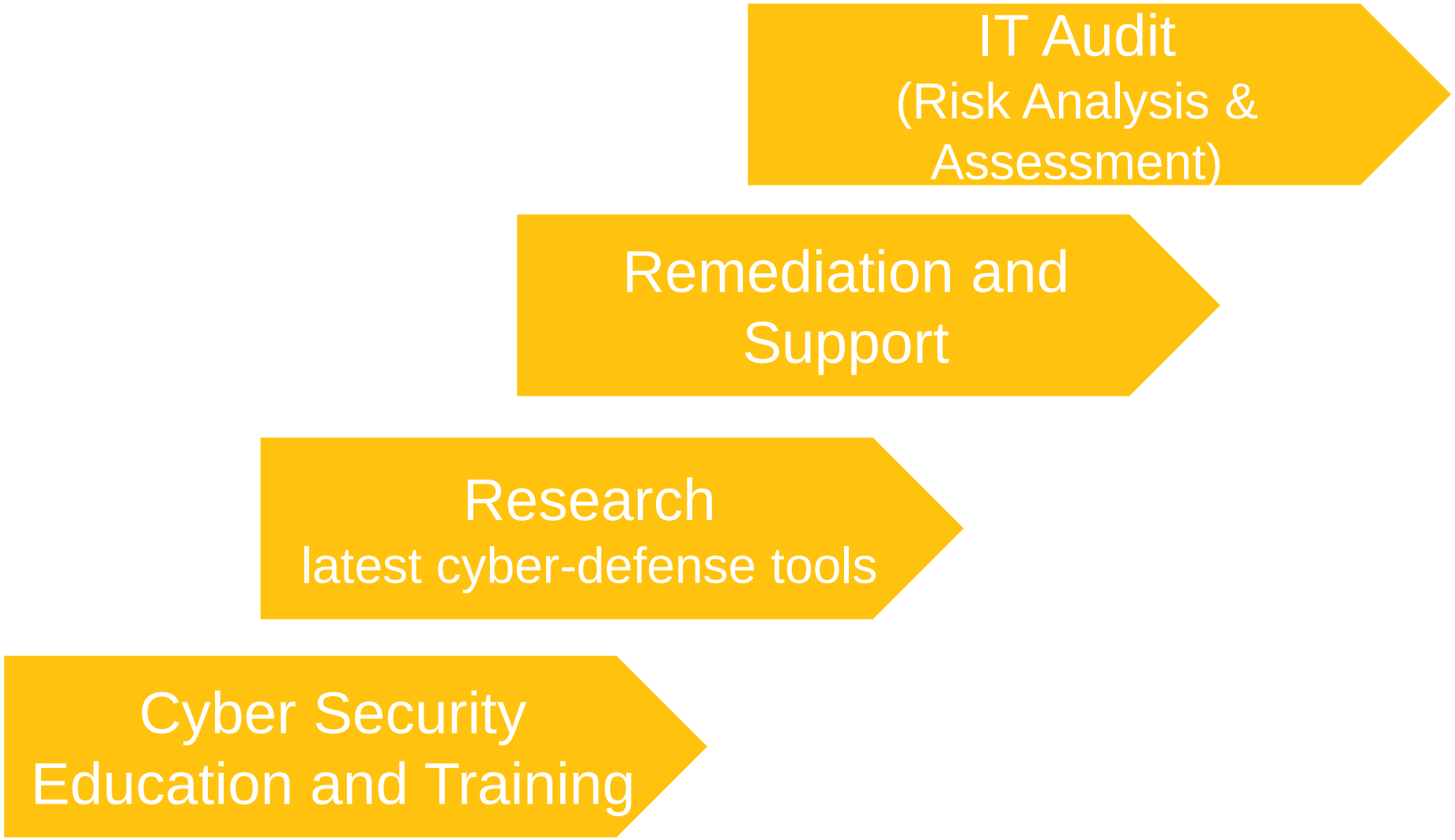
- Preparation
- Identification
- Containment
- Eradication
- Recovery
- Lessons Learned (follow-up)

GAIN INSIGHT AT THE APPLICATION LEVEL



NETFLOW METADATA TO REGENERATE THE DYNAMICS OF PRODUCTION NETWORKS FOR MORE REALISTIC CYBER RANGE SCENARIOS

Building value with Cyber Ranges



ixia

WHY CYBER RANGES?

- Why do organizations need Cyber Ranges:
  - Constantly test SOC/NOC personnel
  - Test network infrastructure
  - Test security devices/policies
  - Research
- Industry can no longer rely on “On The Job” training and shoulder surfing
- Traditional vendor training focuses on HOW to operate device, not HOW TO REACT and DAY TO DAY OPERATION

WHO NEEDS A CYBER RANGE?

- Enterprises
- Service Providers
- Network Equipment Manufacturers
- Government organizations

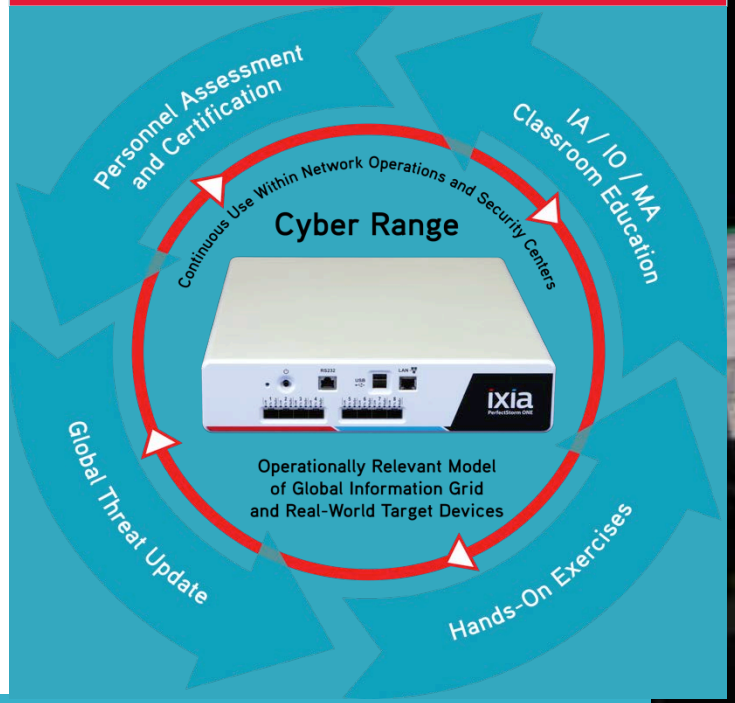
ixia

Cyber Attack Readiness – How a Cyber Range Solution Can Help

Remarkably like your production network

A sandbox to test network infrastructure without causing problems on production network

Puts people under test



BOEING

cisco TOMORROW starts here.

BAE SYSTEMS

LOUISIANA NATIONAL GUARD PROTECT WHAT MATTERS

NORTHROP GRUMMAN

DEPARTMENT OF DEFENSE UNITED STATES OF AMERICA

Ixia Cyber Range Solution

Training Services

Cyber Attack Tools

Cyber Warfare Scenarios

Network Infrastructure Model

Network Traffic Visibility

Internet-Scale Cyber Range Environment

- Realistic target simulations
- Realistic exploit simulations
- Realistic evasion simulations
- Realistic traffic simulation
- Population and country user base
- Mobile subscriber user base
- Data of interest or “needle in a haystack” for data loss prevention (DLP)
- Enterprise and IT services
- Internet IPv4 and IPv6 infrastructure

http://thehackernews.com/2016/09/ddos-attack-iot.html

ixia

Thank you

alenache@ixiacom.com